SG-5110 Gateway Command Line Interface Reference Guide

Model: SG-5110

CLI REFERENCE GUIDE

Contents

Chapter 1 Application Acceleration Configuration Commands

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

1 VWAN Commands

1.1 access-list

Use this command to associate an ACL, so that multilink bundling is not performed on data flows of some users in a branch that are used for accessing servers.

access-list *acl-num*

Use the **no** form of this command to cancel ACL association.

no access-list

Parameter Description

Parameter	Description
acl-num	Indicates the serial number of the ACL to be associated.

Defaults N/A

Command Mode Configuration mode of a VWAN channel in active mode

14

Usage Guide An ACL does not need to be configured. An ACL ensures that multilink bundling is not performed on data flows of some users in a branch that are used for accessing servers.

Configuration Example #Associate an ACL in VWAN channel mode of a branch, to ensure that multilink bundling is not performed on data flows of some users in the branch that are used for accessing servers.

```
FS(config)# vwan channel active CompanyA
FS(config-vwan-channel)# access-list 100
```

Verification Run the **show vwan channel** command to display the ACL associated with the VWAN channel.

N/A

N/A

N/A

1.2 comment

Use this command to comment a VWAN channel with a branch name.

comment *name*

Use the **no** form of this command to cancel the branch name comment for a VWAN channel.

no comment

Parameter Description

Parameter	Description
name	Indicates the name of a branch. It contains a maximum of 31 bytes.

Defaults N/A

Command Mode Configuration mode of a VWAN channel in active mode

14

Usage Guide Comment a VWAN channel with a branch name. 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 in the headquarters for identification.

Configuration Example #Comment a VWAN channel with a branch name.

```
FS(config)# vwan channel active CompanyA
FS(config-vwan-channel)# comment BranchA
```

Verification Run the **show vwan channel** command on the device in the headquarters to check whether the device in the branch correctly advertises its branch name through the VWAN channel.

N/A

N/A

N/A

1.3 limit

Use this command to limit the number of channels that can be configured in a VWAN channel in passive mode.

limit *channel-num*

Use the **no** form of this command to restore the default configuration.

no limit

Parameter Description

Parameter	Description
channel-num	Limits the number of channels that can be configured in a VWAN channel in passive mode.

Defaults 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

14

Usage Guide The number of channels that can be configured in a VWAN channel in passive mode does not need to be configured. You can limit the number of channels that can be configured in each VWAN channel in passive mode when multiple VWAN channels in passive mode are created on the device in the headquarters and the number of devices in branches connected to each VWAN channel needs to be limited, so as to ensure that the device in the headquarters can establish connections with devices in branches through other VWAN channels. The total number of devices in branches connected to VWAN channels in passive mode should be smaller than the number of VWAN channels supported by the device in the headquarters.

Configuration Example #Create two VWAN channels in passive mode to limit the number of channels that can be configured in a VWAN channel in passive mode to 30.

```
FS(config)# vwan channel passive CompanyA
FS(config-vwan-channel)# limit 30
FS(config)# vwan channel passive CompanyB
FS(config-vwan-channel)# limit 30
```

Verification Run the **show vwan channel** command to display the limited number of channels that can be configured in a VWAN channel in passive mode.

N/A

N/A

N/A

1.4 link

Use this command to configure a virtual link in active mode.

link *interface-name* [*source-port*] *dest-ip* [*dest-port*] [**bandwidth** *bandwidth*]

Use the **no** form of this command to delete a virtual link in active mode.

no link *interface-name* [*source-port*] *dest-ip* [*dest-port*] [**bandwidth** *bandwidth*]

Parameter Description

Parameter	Description
interface-name	Indicates the local device port of a virtual link.
source-port	Indicates the UDP source port used by the Multilink Protocol (MP). It does not need to be configured. The default port is Port 12315.
dest-ip	Indicates the peer IP address of the virtual link, that is, the master IP address of the peer device port.

dest -port	Indicates the UDP destination port used by the MP. It does not need to be configured. The default port is Port 12315.
bandwidth *bandwidth*	Indicates the link bandwidth in kbps. It does not need to be configured. By default, it is the same as the bandwidth configured in interface configuration mode.

Defaults N/A

Command Mode Configuration mode of a VWAN channel in active mode

14

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 local 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.

Configuration Example #Create a virtual link in active mode.

```
FS(config)# vwan channel active CompanyA
FS(config-vwan-channel)# link GigabitEthernet 0/1 100.1.1.10
```

Verification Run the **show vwan link** command to display the created virtual link.

N/A

N/A

1.5 link any

Use this command to configure a virtual link in passive mode.

link *interface-name* [*source-port*] **any**

Use the **no** form of this command to delete a virtual link in passive mode.

no link *interface-name* [*source-port*] **any**

Parameter Description

Parameter	Description
interface-name	Indicates the local device port of a virtual link.
source-port	Indicates the UDP source port used by the MP. It does not need to be configured. The default port is Port 12315.

Defaults N/A

Command Mode Configuration mode of a VWAN channel in passive mode

14

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.

Configuration Example #Create a virtual link in passive mode.

```
FS(config)# vwan channel passive CompanyA
FS(config-vwan-channel)# link GigabitEthernet 0/1 any
```

Verification Run the **show vwan link** command to display the created virtual link.

N/A

N/A

1.6 server

Use this command to configure a server address.

server *server-ip* [**tcp** *tcp-port* | **udp** *udp-port*]

Use the **no** form of this command to cancel the server address.

no server *server-ip* [**tcp** *tcp-port* | **udp** *udp-port*]

Parameter Description

Parameter	Description
server-ip	Indicates the server IP address. It is usually set to the IP address obtained after NAT static mapping or port mapping is performed.
tcp *tcp-port*	Indicates the TCP server port configured on the device.
udp *udp-port*	Indicates the UDP server port configured on the device.

Defaults N/A

Command Mode Configuration mode of a VWAN channel in passive mode

14

Usage Guide The TCP port and UDP port do not need to be specified. You can run the **ping** command to detect the connectivity between PCs in a branch and a server. 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.

Configuration Example

#Map the video server in the headquarters to 100.1.1.11 in NAT static mapping mode and configure the address of the video server in a VWAN channel in the headquarters.

```
FS(config)# vwan channel passive CompanyA
FS(config-vwan-channel)# server 100.1.1.11
```

Verification

1. Run the **show running** command on the device in the headquarters to display the configured server address.

2. Run the **show vwan channel servers** command on the device in the branch to display the server address pushed by the device in the headquarters.

1.7 show vwan channel

Use this command to display information about a VWAN channel.

show vwan channel

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

2

Usage Guide

This command displays information about a VWAN channel, including the status and name of the VWAN channel, branch name of the peer device, serial number of the associated ACL, and number of transmitted and received packets. The status shows whether the VWAN channel is successfully established.

Configuration Example

#Display information about a VWAN channel.

```
FS#show vwan channel
ID             name        state      acl loss_recov link_num send_pkts send_bytes recv_pkts recv_bytes comment
estab_time
0x22342600 CompanyA ESTABED 0     1              2           0            0             0            0
BranchA 2013-7-15 10:00:00
```

Field description:

Field	Description
ID	Indicates the internally used ID of a VWAN channel.
name	Indicates the name of a VWAN channel.
state	Indicates the state of a VWAN channel, which may be opened, established, or closed.
acl	Indicates the serial number of the associated ACL. The value **0** indicates no association.

link_num	Indicates the number of virtual links in a VWAN channel.
send_pkts	Indicates the number of sent packets.
send_bytes	Indicates the number of bytes of sent packets.
recv_pkts	Indicates the number of received packets.
recv_bytes	Indicates the number of bytes of received packets.
comment	Indicates the branch name advertised by the peer device.
estab_time	Indicates the establishment time of the VWAN channel.

N/A

N/A

1.8 show vwan channel servers

Use this command to display the list of server addresses pushed by the peer device.

show vwan channel servers

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

2

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.

Configuration Example

#On the device in a branch, check the list of server addresses pushed by the device in the headquarters.

```
FS#show vwan channel servers
channel: CompanyA, peer-num: 2
      ip                    proto      port
   1. 100.1.1.11          0          0
   2. 100.1.1.12          0          0
```

Field description:

Field	Description
Channel	Indicates the name of a VWAN channel.
peer-num	Indicates the number of server addresses pushed by the peer device.
ip	Indicates the server IP address.

proto	Indicates the protocol applied to the server, TCP or UDP. The value **0** indicates that no protocol is specified.
port	Indicates the server port, to which the protocol is applied. The value **0** indicates that no port is specified.

N/A

N/A

1.9 show vwan link

Use this command to display information about a virtual link.

show vwan link

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

2

Usage Guide

This command displays information about a virtual link, including 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.

Configuration Example

#Display information about a virtual link.

```
FS#show vwan link
ID          channel      intf_name               local IP     sport peer IP      dport bw     state            send_pkts
send_bytes recv_pkts recv_bytes
0x26ebd7 0x22342600 GigabitEthernet 0/1 120.1.1.20 12315 100.1.1.10 12315 2000 established 19147          766028
19130        765240
0x27d913 0x22342600 GigabitEthernet 0/2 220.1.1.20 12315 200.1.1.10 12315 2000 established 19147          766048
19129        765188
```

Field description:

Field	Description
ID	Indicates the internally used ID of a virtual link.
channel	Indicates the internally used ID of a VWAN channel to which the virtual link belongs.
intf_name	Indicates the name of a local interface.
local IP	Indicates the local IP address.
sport	Indicates the local UDP port.

peer IP	Indicates the peer IP address.
dport	Indicates the peer UDP port.
bw	Indicates the bandwidth of the virtual link.
state	Indicates the state of the virtual link, which may be free, connecting, established, fault, closing, or listen.
send_pkts	Indicates the number of sent packets.
send_bytes	Indicates the number of bytes of sent packets.
recv_pkts	Indicates the number of received packets.
recv_bytes	Indicates the number of bytes of received packets.

N/A

N/A

1.10 show vwan flowrate

Use this command to display traffic information of a VWAN channel.

show vwan flowrate [cha*nnel-id*]

Parameter Description

Parameter	Description
channel-id	Indicates the ID of a VWAN channel. If the VWAN channel ID is not specified, information about accumulated traffic of all VWAN channels is displayed. The value range is from 1 to 4,294,967,295.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

2

Usage Guide Check traffic information about a VWAN channel, so as to judge whether data flows of users in a branch who access servers in the headquarters are successfully transmitted via the VWAN channel.

Configuration Example #Display traffic information of a VWAN channel.

```
FS#show vwan flowrate
up-all     down-all up-rate down-rate
1132800 3332800     3600         8700
```

Field description:

Field	Description
up-all	Indicates the number of accumulated bytes in the uplink direction.
down-all	Indicates the number of accumulated bytes in the downlink direction.

up-rate	Indicates the uplink traffic in bps.
down-rate	Indicates the downlink traffic in bps.

N/A

N/A

1.11 vwan channel

Use this command to configure a VWAN channel.

vwan channel [**passive | active**] *channel-name*

Use the **no** form of this command to delete a VWAN channel.

no vwan channel [**passive** | **active**] *channel-name*

Parameter Description

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 bytes.

Defaults N/A

Command Mode Global configuration mode

14

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 devices in branches. Ensure that names at both ends of a VWAN channel are consistent.

Configuration Example

#Configure a VWAN channel in passive mode.

```
FS(config)# vwan channel passive CompanyA
```

#Configure a VWAN channel in active mode.

```
FS(config)# vwan channel active CompanyA
```

Verification Run the **show vwan channel** command to display created VWAN channels.

1.12 vwan enable

Use this command to enable multilink bundling.

vwan enable

Use the **no** form of this command to disable multilink bundling.

no vwan enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Multilink bundling is disabled by default.

Command Mode Global configuration mode

14

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

Configuration Example #Enable multilink bundling.

```
FS(config)# vwan enable
```

Verification Run the **show running** command to check whether multilink bundling is enabled.

N/A

N/A

N/A

1.13 vwan mss

Use this command to change the value of the TCP MSS field to a specified value for multilink bundling.

vwan mss *mss-val*

Use the **no** form of this command to cancel the configuration.

no vwan mss

Parameter Description

Parameter	Description
mss-val	Specifies the value of the MSS field. If the value of the MSS field in TCP SYN packets is greater than the specified value, change the value of the MSS field. The value range is from 500 to 1,460.

Defaults N/A

Command Mode Global configuration mode

14

Usage Guide The value of the MSS field does not need to be configured. Bytes added due to MP encapsulation and FEC encapsulation are automatically removed from the value of the MSS field.

Configuration Example N/A

Verification Run the **show running** command to display the configured value of the MSS field.

N/A

N/A

N/A

2 HTTP-AD Commands

2.1 was enable

Use this command to enable the WAS module.

was enable

Use the **no** form of this command to disable the WAS module.

no was enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The WAS module is enabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the WAS module.

Configuration Example The following example enables the WAS module.

```
FS(config)# was enable
```

Verification Run the **show was status** command to check whether the WAS module is enabled or disabled.

2.2 was http ad enable

Use this command to enable the moving ad function.

was http ad enable

Use the **no** form of this command to disable the moving ad function.

no was http ad enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The moving ad function is enabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the moving ad function.

Configuration Example The following example enables the moving ad function.

```
FS(config)# was http ad enable
```

Verification Run the **show was http ad config** command to check whether the moving ad function is enabled or disabled.

2.3 was http ad url

Use this command to configure the URL of an ad script to be inserted.

was http ad url *string*

Use the **no** form of this command to delete the URL of the ad script.

no was http ad url

Parameter Description

Parameter	Description
string	URL of the ad script

Defaults N/A

Command Mode Global configuration mode

Usage Guide The ad script is provided by the network operator.

ℹ Some scripts may cause the problem that the display on some Web pages is abnormal or some Web pages are not displayed.

Configuration Example The following example configures the URL of the ad script of the network operator.

```
FS(config)# was http ad url http://rujie.com.cn/ad.js
```

Verification Run the **show was http ad config** command to check the script link.

2.4 in-path rule auto-discovery dstport port 80 accelerate http rulenum start

Use this command to configure the Port 80-based TCP proxy rule.

in-path rule auto-discovery dstport port 80 accelerate http rulenum start

Use the **no** form of this command to delete the TCP proxy rule.

no in-path rule all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Enable the Port 80-based TCP proxy.

Configuration Example

The following example enables the Port 80-based TCP proxy.

```
FS(config)# in-path rule auto-discovery dstport port 80 accelerate http rulenum start
```

Verification

Run the **show in-path rules** command to check the TCP proxy rule.

2.5 show was status

Use this command to display the status of the WAS module.

show was status

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to display the running status of the WAS module.

Configuration Example

The following example displays the running status of the WAS module.

```
FS# show was status
was:on
```

2.6 show was http ad config

Use this command to display the current configuration of the moving ad function.

show was http ad config

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to display the configuration information of the moving ad function.

Configuration Example

The following example displays the configuration information of the moving ad function.

```
FS#show was http ad config
ad    status : on
ad    url       : http://rujie.com.cn/ad.js
```

2.7 show was http ad status

Use this command to display the current running status of the moving ad function.

show was http ad status

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to check the current running status of the moving ad function.

Configuration Example

The following example displays the current running status of the moving ad function.

```
FS# show was http ad status
ad      status : on
Http request count                  : 9
Http insert ad count                : 0
Http insert html count              : 0
Http insert ad rate                 : 0%
Http no 200 response                : 0
Http exceed memory count            : 0
Http no html feature                : 0
Http other fail count               : 0
Http decprs count                   : 0
Http decprs success count           : 0
Http decprs gzip off count          : 0
Http decprs fail count              : 0
Http decprs no html count           : 0
Http decprs abnor       count       : 0
Http avg memory                     : 0
```

2.8 show in-path rules

Use this command to display the TCP proxy rule.

show in-path rules

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide Use this command to check the TCP proxy rule.

Configuration Example The following example displays the TCP proxy rule.

```
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
```

3 APP-CACHE Commands

3.1 was http app-cache enable

Use this command to enable APP-CACHE. Use the **no** form of this command to disable APP-CACHE.

was http app-cache enable

no was http app-cache enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to enable APP-CACHE.

Configuration Examples

N/A

Verification

Run the **show was http app-cache config** command to check whether the configuration takes effect.

```
FS#show was http app-cache config
app-cache : on
```

Prompt Message

N/A

Common Errors

The WAS module is disabled.

3.2 was http app-cache rule

Use this command to configure the APP-CACHE matching rule. Use the **no** form of this command to delete the APP-CACHE matching rule.

was http app-cache rule { **type** | **key** } *string*

no was http app-cache rule { **type** | **key** } *string*

Parameter Description

Parameter	Description
type *string*	Indicates the type of matched file. The default value is **apk|ipa**, and regular expressions are supported.
key *string*	Indicates the URL matching rule. The URL can be broken into the elements of $host, $path, $name, and $args, which can be combined.

Defaults

The default value of rule type is **ipa|apk**.

The default value of rule key is **$path$name**.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to determine whether to cache an HTTP packet based on the configured rule.

1. According to the default rule, only APK and IPA files are cached.
2. The index value algorithm determining whether to cache files adopts the path and name sections of an URL.

Downloaded files not matching the rule are not cached.

Configuration Examples

1. The following example caches only Apple IPA files. (IPA and APK files are cached by default.)

```
FS(config)# was http app-cache rule type ipa
```

2. The following example focuses only on the file name, regardless of the URL and other elements.

```
FS(config)# was http app-cache rule key $name
```

Verification

1. Run the **show was http app-cache config** command to check the configuration.
2. Perform app download operation and check whether the cache rule takes effect.

3.3 was http inpath domain

Use this command to configure a domain name to generate the dynamic inpath rule of a TCP proxy. Use the **no** form of this command to delete the configuration.

was http inpath domain *string*

no was http inpath domain *string*

Parameter Description

Parameter	Description
string	Indicates the domain name or IP address.

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

After the configuration, TCP streams for accessing the server enter the TCP proxy and the APP-CACHE module.

If a domain name is configured, the DNS server needs to be set.

Configuration Examples

1. The following example configures streams for accessing Apple Store to enter APP-CACHE.

```
FS(config)# was http inpath domain ituns.apple.com
```

2. The following example configures streams for accessing 10.0.0.10 to enter APP-CACHE.

```
FS(config)# was http inpath domain 10.0.0.10
```

Verification

1. Run the **show was http inpath domain** command.

2. Perform the download operation, and check whether streams for accessing the corresponding server enter the TCP proxy.

3.4 was http app-cache url

Use this command to configure the redirection URL of a specified app to be cached by APP-CACHE. Use the **no** form of this command to delete the redirection URL of a specified app to be cached by APP-CACHE.

was http app-cache url *string*

no was http app-cache url *num*

no was http app-cache url *all*

Parameter Description

Parameter	Description
string	Indicates the redirection URL of a specified app. Only app files downloaded within 10 minutes after access to the redirection URL are cached.
num	Deletes the No. of the redirection URL.
all	Deletes all redirection URLs

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide

After the configuration, TCP streams for accessing the server enter the TCP proxy and the APP-CACHE module.

App files downloaded within 10 minutes after access to the URL are cached.

ⓘ If the host section in the URL is a domain name, the DNS server needs to be configured.

Configuration Examples

The following example designates the download page of a vendor's app.

```
FS(config)# was http app-cache url http://rujie.com.cn/appdownload.html
```

Verification

1. Run the **show was http app-cache config** command to check the configuration.

2. Access the configured URL and download an app.

3.5 was http app-cache match url

Use this command to configure the URL characteristic string for a designated app to be cached by APP-CACHE. Use the **no** form of this command to delete the URL characteristic string of a designated app to be cached by APP-CACHE.

was http app-cache match url *string*

no was http app-cache match url *string*

no was http app-cache match url *all*

Parameter Description

Parameter	Description
string	Indicates the characteristic string, used for matching the URL.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide After this command is configured, the URL and the characteristic string are compared during resource access. The resource is cached only when the URL and the characteristic string match each other.

If the host section in the URL is a domain name, the DNS server needs to be configured.

Configuration Examples The following example configures the URL characteristic string for a designated app.

```
FS(config)# was http app-cache match test.com
FS(config)# was http app-cache match qq
FS(config)# was http app-cache match 360
```

Verification 1. Run the **show was http app-cache config** command to check the configuration.

2. Download an app, and verify that the designated app file is cached based on matching of the URL characteristic string.

3.6 was http app-cache match app-name

Use this command to configure the app name characteristic string for a designated app to be cached by APP-CACHE. Use the **no** form of this command to delete the app name characteristic string of a designated app to be cached by APP-CACHE.

was http app-cache match app-name *string*

no was http app-cache match app-name

Parameter Description

Parameter	Description
string	Indicates the characteristic string, used for matching the app name.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide After this command is configured, the app name and the characteristic string are compared during resource access. The resource is cached only when the app name and the characteristic string match each other.

ⓘ If the host section in the URL is a domain name, the DNS server needs to be configured.

Configuration Examples The following example designates the download page of a vendor's app.

```
FS(config)# was http app-cache match app-name abc.app
FS(config)# was http app-cache match app-name abc.apk
```

Verification 1. Run the **show was http app-cache config** command to check the configuration.

2. Download an app and verify that cache is performed according to the configured app name characteristic string.

3.7 clear was http app-cache database

Use this command to clear cached files.

clear was http app-cache database

Parameter Description

Parameter	Description
N/A	

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to clear downloaded cache files to release disk space.

Configuration Examples The following example clears downloaded cache files to release disk space.

```
FS(config)# clear was http app-cache database
```

Verification Run the **show was http app-cache status** command to check the disk space.

3.8 show was http app-cache database

Use this command to display information about files currently cached by APP-CACHE.

show was http app-cache database num

Parameter Description

Parameter	Description
num	Indicates the number of to-be-displayed entries.

Command Privileged EXEC mode, global configuration mode, and interface configuration mode

Mode

Default Level 14

Usage Guide This command is used to display information about files currently cached by APP-CACHE.

3.9 show was http app-cache config

Use this command to display current configuration of APP-CACHE.

show was http app-cache config

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide This command is used to display the configuration of APP-CACHE.

3.10 show was http app-cache status

Use this command to display current running status of all APP-CACHE modules.

show was http app-cache status

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide

Configuration Examples The following example displays current running status of all APP-CACHE modules.

```
FS#show was http app-cache status
app-cache : on

Http request count              : 1021
Http Cache hit count          : 0
Http Cache hit rate             : 0%
Http is_cacheable count    : 1
Http is_cacheble rate        : 0%
Http Cache count                  : 787

Http app_cache cache total size      : 100.00GB
Http app_cache cache used    size      : 14.73MB
Http app_cache cache left    size      : 99.99GB



Cache disk space info:
Total_size                          : 300452.93MB
Disk_available                    : 283145.84MB
```

3.11 show was http app-cache muldownload status

Use this command to display information about files downloaded in multi-threaded manner.

show was http app-cache muldownload status

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

Configuration Examples

The following example displays information about files downloaded in multi-threaded manner.

```
FS#show was http app-cache muldownload status
filename                                                          size
   0b668ba1018def125c15f3760b2aa347         7804576
0b668ba1018def125c15f3760b2aa347-tmp:
   s138-23792520-41878397-133826528         9223807
   s141-41878398-75311012-133826528         7093886
   s140-75311013-131729375-133826528         9868573
   s139-112418973-131729375-133826528         6274685
   e139-131729376-132777951-133826528         1048576
   e138-132777952-133826527-133826528         1048576
```

3.12 show was http inpath domain

Use this command to display the domain name resolution status of APP-CACHE.

show was http inpath domain

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

Run the **show was http inpath domain** command to display the current configuration and the IP address resolved by the DNS server.

Configuration Examples

The following example displays the domain name resolution status of APP-CACHE.

```
FS# show was http inpath domain
0       domain: www.baidu.com
        0           14.215.177.37
        1           14.215.177.38
FS#
```

3.13 was http storage usb

Use this command to store cached files in the USB flash drive. Use the **no** form of this command to stop storing cached files in the USB flash drive.

was http storage usb

no was http storage usb

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to store cached files in the USB flash drive, thereby implementing capacity expansion.

Configuration Examples

N/A

Verification

Run the **show was http storage config** command to check whether the configuration takes effect.

```
FS# show was http storage config
Usb extend                    : on
```

Common Errors

The USB flash drive does not exist or is incorrectly formatted.

3.14 was httpd enable

Use this command to enable the HTTP download service of APP-CACHE. Use the **no** form of this command to disable the HTTP download service of APP-CACHE.

was httpd enable

no was httpd enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to enable the HTTP download service of APP-CACHE.

Configuration Examples

N/A

Verification

Run the **show was httpd config** command to check whether the configuration takes effect.

```
FS# show was httpd config
was httpd enable                        : on
was httpd port                          : 6080
```

Common Errors

The WAS module is disabled.

3.15 was httpd hot-html-generate app-cahce

Use this command to generate a resource list file.

was httpd hot-html-generate app-cahce filter *string1* **filename** *string2*

Parameter Description

Parameter	Description
string1	Indicates the filtering criteria, for example, ipa|apk.
string2	Indicates the file name.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide

1. Run the **show was httpd hot-html database** *num* command to display currently generated files.

Configuration Examples The following example generates a resource list file.

```
FS# was http hot-html-generate app-cache
Create hot html succ url: http://127.0.0.1:6080/hot_html/appc-cache-hot.html
```

3.16 show was httpd config

Use this command to display configuration of the HTTP download service of APP-CACHE.

show was httpd config

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide This command is used to display the configuration of APP-CACHE.

3.17 show was httpd hot-html database

Use this command to display the generated cached resource list file.

show was httpd hot-html database *num*

Parameter Description

Parameter	Description
num	Indicates the number of to-be-displayed entries.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide This command is used to display the generated cached resource list file.

3.18 clear was httpd hot-html database

Use this command to clear cached files.

clear was http hot-html database

Parameter Description

Parameter	Description
N/A	

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to clear all resource list files.

Configuration Examples The following example clears resource list files to release disk space.

```
FS# clear was http hot-html database
```

Verification Run the **show was httpd hot-html database** command for a check.

Chapter 2 Basic Configuration Commands

1 Command Line Interface Commands

1.1 alias

Use this command to configure a command alias in global configuration mode. Use the **no** form of this command to restore the default setting.

alias *mode command-alias original-command*

no alias *mode command-alias*

Parameter Description

Parameter	Description
mode	Mode of the command represented by the alias
command-alias	Command alias
original-command	Syntax of the command represented by the alias

Defaults Some commands in user or privileged EXEC mode have default alias.

Command Mode Global configuration mode.

Usage Guide The following table lists the default alias of the commands in privileged EXEC mode.

Alias	Actual Command
h	help
p	ping
s	show
u	undebug
un	undebug

The default alias cannot be removed by the **no alias exec** command.

After configuring the alias, you can use a word to replace a command. For example, you can create an alias to represent the first part of a command, and then type the rest part of the command.

The mode of the command represented by the alias is the command mode existing in the current system. In the global configuration mode, you can use the **alias ?** command to list all the modes under which you can configure alias for commands.

```
FS(config)# alias ?
  aaa-gs                     AAA server group mode
  acl                         acl configure mode
  config                     globle configure mode
......
```

The alias also has its help information that is displayed after * in the following format:

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

For example, in the privileged EXEC mode, the default alias s stands for show. You can enter s? to query the key words beginning with s and the help information of the alias.

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

If an alias represents more than one word, the command will be displayed in brackets. For example, if you set sv stand for show version in the privileged EXEC mode, then:

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

The alias must begin with the first letter of the command. The first letter of the command cannot be a space. The space before the command cannot be used as a valid alias.

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

The command alias also has its help information. For example, if the alias ia represents ip address in the interface configuration mode, then:

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

The above help information lists the parameters of **ip address** and shows the actual command name.

You must enter an entire alias; otherwise it cannot be recognized.

Use the **show aliases** command to show the aliases setting in the system.

Configuration Examples

The following example uses def-route to represent the default route setting of ip route 0.0.0.0 0.0.0.0 192.168.1.1 in the global configuration mode:

```
FS# configure terminal
FS(config)# alias config def-route ip route 0.0.0.0 0.0.0.0 192.168.1.1
FS(config)#def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
FS(config)# end
FS# show aliases config
globle configure mode alias:
def-route                    ip route 0.0.0.0 0.0.0.0
192.168.1.1
```

Related Commands

Command	Description
show aliases	Displays the aliases settings.

Platform Description

N/A

1.2 privilege

Use this command to attribute the execution rights of a command to a command level in global configuration mode. Use the **no** form of this command to restore the default setting.

privilege *mode* [**all**] [**level** *level* **|** **reset**] *command-string*

no privilege *mode* [**all**] [**level** *level*] *command-string*

Parameter Description

Parameter	Description
mode	CLI mode of the command to which the execution rights are attributed.
all	Command alias
level *level*	Specifies the execution right levels (0–15) of a command or sub-commands
reset	Restores the command execution rights to its default level
command-string:	Command string to be authorized

Defaults N/A

Command Mode Global configuration mode.

Usage Guide The following table lists some key words that can be authorized by the **privilege** command in CLI mode. The number of command modes that can be authorized may vary with different devices. In the global configuration mode, you can use the **privilege ?** command to list all CLI command modes that can be authorized.

Mode	Descripton
config	Global configuration mode.
exec	Privileged EXEC mode
interface	Interface configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
keychain	KeyChain configuration mode
keychain-key	KeyChain-key configuration mode

Configuration Examples The following example sets the password of CLI level 1 as **test** and attribute the **reload** rights to reset the device:

```
FS(config)#privilege exec level 1 reload
```

You can access the CLI window as level-1 user to usef the **reload** command:

```
FS>reload ?
LINE      Reason for reload
```

<cr>   You can use the key word **all** to attribute all sub-commands of reload to level-1 users:

```
FS(config)# privilege exec all level 1 reload
```

After the above setting, you can access the CLI window as level-1 user to use all sub commands of the **reload** command:

```
FS>reload ?
LINE      Reason for reload
at                       reload at a specific time/date
cancel                 cancel pending reload scheme
in                       reload after a time interval
```

```
<cr>
```

Related Commands

Command	Description
enable secret	Sets the CLI-level password.

Platform Description N/A.

1.3 show aliases

Use this command to show all the command aliases or aliases in special command modes.

show aliases [*mode*]

Parameter Description

Parameter	Description
mode	Mode of the command represented by the alias.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide This command displays the configuration of all aliases if no command mode is input.

Configuration Examples The following example displays the command alias in privileged EXEC mode:

```
FS#show aliases exec
exec mode alias:
h                    help
p                    ping
s                    show
u                    undebug
un                   undebug
```

Related Commands

Command	Description
alias	Sets a command alias.

Platform Description N/A.

2 Basic Configuration Management Commands

2.1 <1-99>

Use this command to restore the suspended Telnet Client session.

<1-99>

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

User EXEC mode

Usage Guide

This command is used to restore the suspended Telnet Client session. Hot keys (ctrl+shift+6 x) are used to exit the Telnet Client session creation. The **<1-99>** command is used to restore the session. If the session is created, you can use the **show session** command to display the session.

Configuration Examples

The following example restores the suspended Telnet Client session.

```
FS# 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.2 banner exec

Use this command to configure a message to welcome the user entering user EXEC mode through the line. Use the **no** form of this command to restore the default setting.

banner exec *c message c*

no banner exec

Parameter Description

Parameter	Description
c	Separator of the message. Delimiters are not allowed in the message.
message	Contents of the message.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to configure the welcome message. The system discards all the characters next to the terminating symbol.

When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the EXEC message or the incoming message is displayed. If it's a reverse Telnet session, the incoming message is displayed. Otherwise, the EXEC message is displayed.

The messages are for all lines. If you want to disable display the EXEC message on a specific line, configure the **no exec-banner** command on the line.

Configuration Examples

The following example configures a welcome message.

```
FS(config)# banner exec $ Welcome $
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.3 banner incoming

Use this command to configure a prompt message for reverse Telnet session. Use the **no** form of this command to remove the setting.

banner incoming *c message c*

no banner incoming

Parameter Description

Parameter	Description
c	Separator of the message. Delimiters are not allowed in the message.
message	Contents of the message.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to configure a prompt message. The system discards all the characters next to the terminating symbol.

When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the welcome message or the prompt message is displayed. If it's a reverse Telnet session, the prompt message is displayed. Otherwise, the welcome message is displayed.

Configuration Examples

The following example configures a prompt message for reverse Telnet session.

```
FS(config)# banner incoming $ Welcome $
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.4 banner login

Use this command to configure a login banner. Use **no** form of this command to r remove the setting.

banner login *c message c*

no banner login

Parameter Description

Parameter	Description
c	Separator of the message contained in the login banner. Delimiters are not allowed in the MOTD.
message	Contents of the login banner

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command sets the login banner message, which is displayed at login. The system discards all the characters next to the terminating symbol.

Configuration Examples

The following example configures a login banner.

```
FS(config)# banner login $ enter your password $
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.5 banner motd

Use this command to set the Message-of-the-Day (MOTD) . Use the **no** form of this command to remove the setting.

banner [**motd**] *c message c*

no banner [**motd**]

Parameter Description

Parameter	**Description**
c	Separator of the MOTD. Delimiters are not allowed in the MOTD.
message	Contents of an MOTD

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command sets the MOTD, which is displayed at login. The letters that follow the separator will be discarded.

Configuration Examples The following example configures the MOTD.

```
FS(config)# banner motd $ hello,world $
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

2.6 banner prompt-timeout

Use this command to configure the prompt-timeout message to notify timeout. Use the **no** form of this command to remove the setting.

banner prompt-timeout *c message c*

no banner prompt-timeout

Parameter Description

Parameter	**Description**
c	Separator of the message. Delimiters are not allowed in the message.
message	Contents of the message.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The system discards all the characters next to the terminating symbol.

When authentication times out, the banner prompt-timeout message is displayed.

Configuration Examples

The following example configures the prompt-timeout message to notify timeout.

```
FS(config)# banner exec $ authentication timeout $
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.7 banner slip-ppp

Use this command to configure the slip-ppp message for the SLIP/PPP session. Use the **no** form of this command to remove the setting.

banner slip-ppp *c message c*

no banner slip-pp

Parameter Description

Parameter	Description
c	Separator of the message. Delimiters are not allowed in the message.
message	Contents of the message.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to configure the slip-ppp message for the SLIP/PPP session. The system discards all the characters next to the terminating symbol.

When the SLIP/PPP session is created, the slip-ppp message is displayed on the corresponding terminal.

Configuration Examples

The following example configures the banner slip-ppp message for the SLIP/PPP session.

```
FS(config)# banner slip-ppp $ Welcome $
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.8 configure

Use this command to enter global configuration mode.

configure [**terminal**]

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example enters global configuration mode.

```
FS# configure
FS(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.9 disable

Use this command to switch from privileged EXEC mode to user EXEC mode or lower the privilege level.

disable [*privilege-level*]

Parameter Description

Parameter	Description
privilege-level	Privilege level

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to switch to user EXEC mode from privileged EXEC mode. If a new privilege level is added, the current privilege level will be lowered.

ℹ The privilege level that follows the **disable** command must be lower than the current level.

Configuration The following example lowers the current privilege level of the device to level 10.

Examples

```
FS# disable 10
```

Related Commands

Command	Description
enable	Moves from user EXEC mode enter to privileged EXEC mode or reaches a higher level of authority.

Platform Description

N/A

2.10 disconnect

Use this command to disconnect the Telnet Client session.

disconnect *session-id*

Parameter Description

Parameter	Description
session-id	Telnet Client session ID.

Defaults

N/A

Command Mode

User EXEC mode

Usage Guide

This command is used to disconnect the Telnet Client session by setting the session ID.

Configuration Examples

The following example disconnects the Telnet Client session by setting the session ID.

```
FS# disconnect 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.11 do telnet

Use this command to login to Telnet server.

do telnet [**oob**] *host* [*port*] [**/source** { **ip** *A.B.C.D* **|** **ipv6** *X:X:X:X::X* **|** **interface** *interface-name* }]

Parameter Description

Parameter	Description
oob	Connects to Telnet server through oob channel. This parameter is available only when the device has a MGMT port.

host	IPv4 or host name of Telnet server.
port	Configures TCP port ID. The default is 23.
/source	Specifies source IP or source port for Telnet client.
ip *A.B.C.D*	Specifies source IPv4 address for Telnet client.
ipv6 *X:X:X:X::X*	Specifies source IPv6 address for Telnet client.
interface *interface-name*	Specifies source port for Telnet client.

Defaults N/A

Command Mode User EXEC mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.12 enable

Use this command to enter privileged EXEC mode.

enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode N/A

Usage Guide N/A

Configuration Examples N/A

Related

Command	Description

Commands

N/A	N/A

Platform Description

N/A

2.13 enable password

Use this command to configure passwords for different privilege levels. Use the **no** form of this command to restore the default setting.

enable password [**level** *level*] { *password* **|** [**0 | 7**] *encrypted-password* }

no enable password [**level** *leve l*]

Parameter Description

Parameter	Description
password	Password for the user to enter the EXEC configuration layer
level	User's level.
0 | **7**	Password encryption type, "0" for no encryption, "7" for simple encryption (Optional) FS's private algorithm will be used for password encryption. If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted by a FS device.
encrypted-password	Password text.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

No encryption is required in general. The encryption type must be specified for copying and pasting a encrypted password for the device.

A valid password is defined as follows:

- Consists of 1-26 upper/lower case letters and numbers
- Leading spaces are allowed but usually ignored. Spaces in between or at the end are regarded as part of the password.

⚠ If an encryption type is specified and a plaintext password is entered, you cannot enter privileged EXEC mode. A lost password that has been encrypted using any method cannot be restored. In this case, you can only reconfigure the device password.

Configuration Examples

The following example configures the password as **pw10**.

```
FS(config)# enable password pw10
```

Related

Command	Description

Commands

enable secret	Sets the security password

Platform Description N/A

enable secret Sets the security password

2.14 enable secret

Use this command to configure a security password for different privilege levels. Use the **no** form of this command to restore the default setting.

enable secret [**level** ***level***] { ***secret*** | [**0** | **5**] ***encrypted-secret*** }

no enable secret [**level** *level*]

Parameter Description

Parameter	Description
secret	Password for the user to enter the EXEC configuration layer
level	User's level.
0 | **5**	Password encryption type, "0" for no encryption, "5" for security encryption
encrypted-password	Password text

Defaults N/A

Command Mode Global configuration mode

Usage Guide A password comes under two categories: "password" and "security". "Password" indicates a simple password, which can be set only for level 15. "Security" means a security password, which can be set for levels 0-15. If both types of passwords coexist in the system, no "password" type is allowed. If a "password" type password is set for a level other than 15, the system gives an alert and the password is automatically converted into a "security" password. If a "password" type password is set for level 15 and the same as a "security" password, an alert is given. The password must be encrypted, with simple encryption for "password" type passwords and security encryption for "security" type passwords.

Configuration Examples The following example configures the security password as **pw10**.

```
FS(config)# enable secret 0 pw10
```

Related Commands

Command	Description
enable password	Sets passwords for different privilege levels.

Platform Description N/A

2.15 enable service

Use this command to enable or disable a specified service such as **SSH Server/Telnet Server/Web Server/SNMP Agent**.

enable service { **ssh-sesrver** | **telnet-server** | **web-server** [**http | https | all**] | **snmp-agent** }

Parameter Description

Parameter	Description
ssh-server	Enables SSH Server.
telnet-server	Enables Telnet Server.
web-server [**http | https | all**]	Enables HTTP Server.
snmp-agent	Enables SNMP Agent.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Use this command to enable or disable a specified service. Use the **no enable service** command to disable the specified service.

ℹ The **enable service web-server** command is followed by three optional keywords: [http | https | all]. If the command is followed by no keyword or by **all**, the command enables http and https services. Followed by **http**, the command enables http service only. Followed by **https**, the command enables https service only.

Configuration Examples

The following example enables the SSH Server.

```
FS(Config)# enable service ssh-sesrver
```

Related Commands

Command	Description
show service	Displays the service status in the current system.

Platform Description

N/A

2.16 end

Use this command to return to privileged EXEC mode.

end

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

All modes except privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example returns to privileged EXEC mode.

```
FS#con
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#line vty 0
FS(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
FS#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.17 exec-banner

Use this command to enable display of the EXEC message on a specific line. Use the **no** form of this command to restore the default setting.

exec-banner

no exec-banner

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The EXEC message is displayed on all lines by default.

Command Mode

LINE configuration mode

Usage Guide

After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the **no** form of this command on the line.

> This command does not work for the banner incoming message. If you configure the **banner incoming** command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.

Configuration Examples

The following example disables display of the EXEC message on line VTY 1.

```
FS(config)# line vty 1
FS(config-line)no exec-banner
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

2.18 exec-timeout

Use this command to configure connection timeout for this device in LINE mode. Use the **no** form of this command to restore the default setting and the connection never expires.

exec-timeout *minutes* [***seconds***]

no exec-timeout

Parameter Description

Parameter	**Description**
minutes	Timeout in minutes.
seconds	(Optional) Timeout in minutes

Defaults

The default is 10 minutes.

Command Mode

Line configuration mode

Usage Guide

If there is no input or output for this connection within a specified time, this connection will expire, and this LINE will be restored to the free status.

Configuration Examples

The following example sets the connection timeout to 5’30’’.

```
FS(config-line)#exec-timeout 5    30
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

2.19 exit

Use this command to return to the upper configuration mode.

exit

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration Examples

The following example returns to the upper configuration mode.

```
FS#con
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#line vty 0
FS(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
FS#con
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#line vty 0
FS(config-line)#exit
FS(config)#exit
*May 20 09:51:48: %SYS-5-CONFIG_I: Configured from console by console
FS#exit

Press RETURN to get started
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.20 help

Use this command to display the help information.

help

Parameter Description

Parameter	Description
N/A	N/A

Defaults Any mode

Command Mode

Usage Guide This command is used to display brief information about the help system. You can use ”?” to display all commands or a specified command with its parameters.

Configuration Examples The following example displays brief information about the help system.

```
FS#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?'.)
```

The following example displays all available commands in interface configuration mode.

```
FS(config-if-GigabitEthernet 0/0)#?
Interface configuration commands:
   arp                  ARP interface subcommands
   bandwidth            Set bandwidth informational parameter
   carrier-delay        Specify delay for interface transitions
   dampening            Enable event dampening
   default              Set a command to its defaults
   description          Interface specific description
   dldp                 Exec data link detection command
   duplex               Configure duplex operation
   efm                  Config efm for an interface
   end                  Exit from interface configuration mode
   exit                 Exit from interface configuration mode
   expert               Expert extended ACL
   flowcontrol          Set the flow-control value for an interface
   full-duplex          Force full duplex operation
   global               Global ACL
   gvrp                 GVRP configure command
   half-duplex          Force half duplex operation
   help                 Description of the interactive help system
   ip                   Interface Internet Protocol config commands
```

```
  isis              Intermediate System - Intermediate System (IS-IS)
  l2                Config L2 attribute
  label-switching   Enable interface process mpls packet
  lacp              LACP interface subcommands
  lldp              Link Layer Discovery Protocol
  load-interval     Specify interval for load calculation for an interface
  mac               Mac extended ACL
  mac-address       Set mac-address
  mpls              Multi-Protocol Label Switching
  mtu               Set the interface Maximum Transmission Unit (MTU)
  no                Negate a command or set its defaults
  ntp               Configure NTP
  port-group        Aggregateport/port bundling configuration
  redirect          Redirect packets
  rmon              Rmon command
  security          Configure the Security
  show              Show running system information
  shutdown          Shutdown the selected interface
  snmp              Modify SNMP interface parameters
  speed             Configure speed operation
  switchport        Set switching mode characteristics
  vrrp              VRRP interface subcommands
  xconnect          Xconnect commands
```

The following example displays the parameters of a specified command.

```
FS(config)#access-list 1 permit ?
  A.B.C.D   Source address
  any       Any source host
  host      A single source host
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.21 hostname

Use this command to specify or modify the hostname of a device.

hostname *name*

Parameter Description

Parameter	Description
name	Device hostname, string, number or hyphen, up to 63 characters.

Defaults The default is FS.

Command Mode Global configuration mode

Usage Guide This hostname is mainly used to identify the device and is taken as the username for the local device during dialup and CHAP authentication.

Configuration Examples The following example configures the hostname of the device as BeiJingAgenda.

```
FS(config)# hostname BeiJingAgenda
BeiJingAgenda(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.22 ip telnet source-interface

Use this command to configure the IP address of an interface as the source address for Telnet connection.

ip telnet source-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Configures the IP address of the interface as the source address for Telnet connection.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to specify the IP address of an interface as the source address for global Telnet connetction. When using the telnet command to log in a Telnet server, apply the global setting if no source interface or source address is specified. Use the **no ip telnet source-interface** command to restore it to the default setting.

Configuration Examples The following example configures the IP address of the *Loopback1* interface as the source address for global Telnet connection.

```
FS(Config)# ip telnet source-interface Loopback 1
```

Related Commands

Command	Description
telnet	Logs in a Telnet server.

Platform Description

N/A

2.23 lock

Use this command to set a temporary password for the terminal.

lock

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

You can lock the terminal interface and maintain the session continuity to prevent access to the interface by setting a temporary password. Take the following steps to lock the terminal interface:

- Enter the **lock** command, and the system will prompt you for a password:
- Enter the password, which can be any character string. The system will prompt you to confirm the password, clear the screen, and display the "Locked" information.
- To access the terminal, enter the preset temporary password.
- To lock the terminal, run the **lockable** command in line configuration mode and enable terminal locking in the corresponding line.

Configuration Examples

The following example locks a terminal interface.

```
FS(config-line)# lockable
FS(config-line)# end
FS# lock
Password: <password>
Again: <password>
Locked
Password: <password>
FS#
```

Related Commands

Command	Description
lockable	Supports terminal locking in the line.

Platform Description

N/A

2.24 lockable

Use this command to support the **lock** command at the terminal. Use the **no** form of this command to restore the default setting.

lockable

no lockable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

This function is disabled by default.

Usage Guide

This command is used to lock a terminal interface in the corresponding line. To lock the terminal, run the lock command in EXEC mode.

Configuration Examples

The following example enables terminal locking at the console port and locks the console.

```
FS(config)# line console 0
FS(config-line)# lockable
FS(config-line)# end
FS# lock
Password: <password>
Again: <password>
Locked
Password: <password>
```

Related Commands

Command	Description
lock	Locks the terminal.

Platform Description

N/A

2.25 login

Use this command to enable simple login password authentication on the interface if AAA is disabled. Use the **no** form of this command to restore the default setting.

login

no login

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Line configuration mode

Usage Guide

If the AAA security server is inactive, this command enables simple password authentication at login. The password is configured for a VTY or console interface.

Configuration Examples

The following example sets a login password authentication on VTY..

```
FS(config)# no aaa new-model
FS(config)# line vty 0
FS(config-line)# password 0    normatest
FS(config-line)# login
```

Related Commands

Command	Description
password	Configures the line login password

Platform Description

N/A

2.26 login access non-aaa

Use this command to configure non-AAA authentication on line when AAA is enabled. Use the **no f**orm of this command to restore the default setting.

login access non-aaa

no login access non-aaa

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures VTY line authentication with AAA enabled.

```
FS(config)#log access non-aaa
FS(config)#aaa new-model
FS(config)#line vty 0 4
FS(config-line)#login local
FS(config-line)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.27 login authentication

If the AAA is enabled, login authentication must be performed on the AAA server. Use this command to associate login authentication method list. Use the **no** form of this command to restore the default setting.

login authentication { **default |** *list-name* }

no login authentication { **default** | *list-name* }

Parameter Description

Parameter	Description
default	Name of the default authentication method list
list-name	Name of the method list

Defaults

N/A

Command Mode

Line configuration mode

Usage Guide

If the AAA security server is active, this command is used for login authentication using the specified method list.

Configuration Examples

The following example associates the method list on VTY and perform login authentication on a radius server.

```
FS(config)# aaa new-model
FS(config)# aaa authentication login default radius
FS(config)# line vty 0
FS(config-line)# login authentication default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication login	Configures the login authentication method list.

Platform Description N/A

2.28 login local

Use this command to enable local user authentication on the interface if AAA is disabled. Use the **no** form of this command to restore the default setting.

login local

no login local

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Line configuration mode

Usage Guide If the AAA security server is inactive, this command is used for local user login authentication. The user is allowed to use the **username** command.

Configuration Examples The following example sets local user authentication on VTY.

```
FS(config)# no aaa new-model
FS(config)# username    test password 0 test
FS(config)# line vty 0
FS(config-line)# login local
```

Related Commands

Command	Description
username	Configures local user information.

Platform Description N/A

2.29 motd-banner

Use this command to enable display of the MOTD message on a specified line. Use the **no** form of this command to restore the default setting.

motd-banner

no motd-banner

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The MOTD message is displayed on all lines by default.

Command Mode

Line configuration mode

Usage Guide

After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the **no** form of this command on the line.

This command does not work for the incoming message. If you configure the **banner incoming** command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.

Configuration Examples

The following example disables display of the MOTD message on VTY 1.

```
FS(config)# line vty 1
FS(config-line)no motd-banner
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.30 password

Use this command to configure a password for line login, run the **password** command. Use the **no** form of this command to restore the default setting.

password { *password* | [**0** | **7**] *encrypted-password* }

no password

Parameter Description

Parameter	Description
password	Password for remote line login
0|7	Password encryption type, "0" for no encryption, "7" for simple encryption (Optional) FS's private algorithm will be used for password encryption. If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted by a FS device.
encrypted-password	Password text

Defaults

N/A

Command

Line configuration mode

Mode

Usage Guide This command is used to configure a authentication password for remote line login.

Configuration Examples The following example configures the line login password as "red".

```
FS(config)# line vty 0
FS(config-line)# password red
```

Related Commands

Command	Description
login	Moves from user EXEC mode to privileged EXEC mode or enables a higher level of authority.

Platform Description N/A

2.31 prompt

Use this command to set the **prompt** command. Use the **no** form of this command to restore the default setting.

prompt string

Parameter Description

Parameter	Description
string	Character string of the **prompt** command, containing up to 32 letters.

Defaults N/A

Command Mode Global configuration mode

Usage Guide If no prompt string is configured, the system name applies and varies with the system name. The **prompt** command is valid only in EXEC mode.

Configuration Examples The following example sets the prompt string to rgnos.

```
FS(config)# prompt rgnos
FS(config)# end
FSOS
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.32 secret

Use this command to set a password encrypted by irreversible MD5 for line login. Use the **no** form of this command to restore the default setting.

secret { [**0**] *password* | **5** *encrypted-secret* }

no secret

Parameter Description

Parameter	Description
0	(Optional) sets the plaintext password text and encrypts it with irreversible MD5 after configuration.
password	Sets the password plaintext, a string ranging from 1 to 25 characters.
5 *encrypted-secret*	Sets the password text encrypted by irreversible MD5 and saves it as the encrypted password after configuration.

Defaults N/A

Command mode Line configuration mode

Usage Guide This command is used to set a password encrypted by irreversible MD5 that is authenticated by a remote user through line login.

⚠ If the specified encryption type is 5, the logical length of the cipher text to be entered must be 24 and the 1st, 3rd and 8th characters of the password text must be $.

In general, the encryption type does not need to be specified as 5 except when the encrypted password is copied and pasted.

Line mode allows configuration of both “password” and “secret” types passwords at the same time. When the two passwords are the same, the system will send alert notification but the configuration will be permitted. When the system is configured with the two passwords, if the user enters a password that does not match the “secret” type password, it will not continue to match the “password” type password and login fails, enhancing security for the system password.

Configuration Examples The following example sets the password encrypted by irreversible MD5 for line login to vty0.

```
FS(config)# line vty 0
FS(config-line)# secret vty0
```

The following displays the encryption outcome by running the **show** command.

```
secret 5 $1$X834$wvx6y794uAD8svzD
```

Related Commands

Command	Description
login	Sets simple password authentication on the interface as the login authentication mode

Platform Description N/A

2.33 session-timeout

Use this command to configure the session timeout for a remote terminal. Use the **no** form of this command to restore the default setting and the session never expires.

session-timeout *minutes* [**output**]

no session-timeout

Parameter Description

Parameter	Description
minutes	Timeout in minutes.
output	Regards data output as the input to determine whether the session expires.

Defaults The default timeout is 0.

Command Mode LINE configuration mode

Usage Guide If no input or output in current LINE mode is found on the remote terminal for the session within a specified time, this connection will expire, and this LINE will be restored to the free status.

Configuration Examples The following example specifies the timeout as 5 minutes.

```
FS(config-line)#exec-timeout 5 output
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.34 show debugging

Use this command to display debugging state.

show debugging

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration Examples

The following example displays debugging state.

```
FS#show debugging


debug fw-group detect intf-state
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.35 show hostname

Use this command to display the hostname of a device.

show hostname

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the hostname of a device.

```
FS#show hostname
FS
FS#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.36 show line

Use this command to display the configuration of a line.

show line { **console** *line-num* | **vty** *line-num* | *line-num* }

Parameter Description

Parameter	Description
console	Display s the configuration of a console line.
vty	Display s the configuration of a vty line.
line-num	Number of the line.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command displays the configuration of a line.

Configuration Examples

The following example displays the configuration of a console port.

```
FS# show line console 0
CON       Type      speed     Overruns
* 0       CON       9600      45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 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: 53564 bytes
Total output:    395756 bytes
Data overflow:    27697 bytes
stop rx interrupt:    0 times
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.37 show reload

Use this command to display the system restart settings.

show reload

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the restart settings of the system.

Configuration Examples

The following example displays the restart settings of the system.

```
FS# show reload
Reload scheduled in 595 seconds.
At 2003-12-29 11:37:42
Reload reason: test.
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.38 show running-config

Use this command to display how the current device system is configured..

show running-config

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

N/A

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.39 show service

Use this command to display the service status.

show service

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays whether the service is enabled or disabled.

```
FS# show service
web-server       : disabled
web-server(https): disabled
snmp-agent        : enabled
ssh-server        : enabled
telnet-server : disabled
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.40 show sessions

Use this command to display the Telnet Client session information.

show sessions

Parameter

Parameter	Description

Description

N/A	N/A

Defaults

N/A

Command Mode

User EXEC mode

Usage Guide

Telnet Client session information includes the VTY number and the server IP address.

Configuration Examples

The following example displays the Telnet Client session information.

```
FS#show sessions
Conn    Address
*1       127.0.0.1
*2       192.168.21.122
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.41 show startup-config

Use this command to display the device configuration stored in the Non Volatile Random Access Memory (NVRAM).

show startup-config

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

The device configuration stored in the NVRAM is executed while the device is starting.

On a device that does not support **boot config**, **startup-config** is contained in the default configuration file **/config.text** in the built-in flash memory.

On a device that supports **boot config**, configure **startup-config** as follows:

If you have specified a boot configuration file using the **boot config** command and the file exists, **startup-config** is stored in the specified configuration file.

If the boot configuration file you have specified using the **boot config** command does not exist or you have not specified a boot configuration file using the command, **startup-config** is contained in **/config.text** in the built-in flash memory.

Configuration Examples

N/A

Related Commands

Command	Description
boot config	Sets the name of the boot configuration file.

Platform Description

N/A

2.42 show this

Use this command to display effective configuration in the current mode.

show this

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

All modes.

Usage Guide

The configuration in the following range modes cannot be displayed. If the **show this** command is run, the outcome is NULL.

1. Use the **line** *first-line last-line* command to configure lines in a continuous group and enter LINE configuration mode.
2. Use the **vlan range** command to configure VLANs and enter vlan range configuration mode.
3. Use the **interface range** command to configure interfaces and enter interface range configuration mode.

Configuration Examples

```
Use this command to display effective configuration on interface fastEthernet 0/1.FS (config)#interface
fastEthernet 0/1
FS (config-if-FastEthernet 0/1)#show this
Building configuration...
 !
 spanning-tree link-type point-to-point
 spanning-tree mst 0 port-priority 0
 !
```

```
end
FS (config-if-FastEthernet 0/1)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.43 speed

Use this command to set the speed at which the terminal transmits packets. Use the **no** form of this command to restore the default setting.

speed *speed*

no speed

Parameter Description

Parameter	Description
speed	Transmission rate (bps) on the terminal. For serial ports, optional rates include 9600, 19200, 38400, 57600, and 115200 bps. The default rate is 9600 bps.

Defaults

The default is 9600.

Command Mode

Global configuration mode

Usage Guide

This command is used to set the speed at which the terminal transmits packets.

Configuration Examples

The following example sets the rate of the serial port to 57600 bps.

```
FS(config)# line console 0
FS(config-line)# speed 57600
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.44 telnet

Use this command to log in a server that supports telnet connection.

telnet *host* [*port*] [**/source** { **ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* **| interface** *interface-name* }]

Parameter Description

Parameter	Description
Host	The IP address of the host or host name you want to log in.
Port	Selects the TCP port number for login, 23 by default.
/source	Specifies the source IP address or source interface used by the Telnet client.
ip A.B.C.D	Specifies the source IPv4 address used by the Telnet client.
ipv6 *X:X:X:X::X*	Specifies source IPv6 address for Telnet client.
interface *interface-name*	Specifies the source interface used by the Telnet client.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

⚠

Configuration Examples

Related Commands

Command	Description
ip telnet source-interface	Specifies the IP address of the interface as the source address for Telnet connection.
show sessions	Displays the currently established Telnet sessions.
exit	Exits current connection.

Platform Description

N/A

2.45 username

Use this command to set a local username and optional authorization information.. Use the **no** form of this command to restore the default setting.

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*]

no username *name*

Parameter Description

Parameter	Description
name	Username
login mode	Sets 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*	Sets the amount of users online simultaneously.
permission *oper-mode path*	Sets the permission on the specified file. *op-mode* refers to the operation mode and *path* to the file or the directory path.
privilege *privilege-level*	Sets the privilege level, in the range from 0 to 15.
reject remote-login	Confines the account to remote login.
web-auth	Confines the account to web authentication.
pwd-modify	Allows the web authentication user of this account to change the password. It works only when the **web-auth** command is configured.
nopassword	The account is not configured with a password.
password [**0** | **7**] *text-string*	If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted. The password is in plain text by default.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to establish a local user database for authentication.

> If encryption type is 7, the cipher text you enter should contain seven characters to be valid.
> In general, do not set the entryption type 7.
> Instead, specify the type of encryption as 7 only when the encrypted password is copied and pasted.

Configuration Examples

The following example configures a username and password and binds the user to level 15.

```
FS(config)# username test privilege 15 password 0 pw15
```

The following example configures the username and password exclusive to web authentication.

```
FS(config)# username user1 web-auth password 0 pw
```

The following example configures user test with read and write permissions on all files and directories.

```
FS(config)# username test permission rw /
```

The following example configures user test with read, write and execute permissions on all files and directories except the confix.text file.

```
FS(config)# username test permission n /config.text
FS(config)# username test permission rwx /
```

Related Commands

Command	Description
login local	Enables local authentication

Platform Description

N/A

2.46 username export

Use this command to export user information to the file.

username export *filename*

Parameter Description

Parameter	Description
filename	The file name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to export user information to the file.

Configuration Examples The following example exports user information to the file.

```
FS# username export user.csv
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.47 username import

Use this command to import user information from the file.

username import *filename*

Parameter Description

Parameter	Description
filename	The file name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to import user information from the file.

Configuration Examples The following example imports user information from the file.

```
FS# username import user.csv
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.48 write

Use this command to save **running-config** at a specified location.

write [**memory | terminal**]

Parameter Description

Parameter	Description
memory	Writes the system configuration (running-config) into NVRAM, which is equivalent to **copy running-config startup-config**.
terminal	Displays the system configuration, which is equivalent to **show running-config**.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Despite the presence of alternative commands, these commands are widely used and accepted. Therefore, they are reserved to facilitate user operations.

The system automatically creates the specified file and writes it into system configuration if the device that stores the file exists;

The system will ask you whether to save the current configuration in default boot configuration file /config.text and perform an action as required if the device that stores the file does not exist possibly because the boot configuration file is stored on a removable storage device such as USB drive and the device has not been loaded when you run the **write** [**memory**] command.

Configuration Examples

The following example saves **running-config** at a specified location.

```
FS# write
Building configuration...
[OK]
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

3 LINE Commands

3.1 access-class

Use this command to control login into the terminal through IPv4 ACL. Use the **no** form of this command to restore the default setting.

access-class { *access-list-number* | *access-list-name* } { **in | out** }

no access-class { *access-list-number* | *access-list-name* } { **in | out** }

Parameter Description

Parameter	Description
access-list-number	Specifies the ACL number. Standard IP ACL number is from 1 to 99 and from 1300 to 1999. Extended IP ACL number is from 100 to 199 and from 2000 to 2699.
access-list-name	Specifies the ACL name.
in	Filters the incoming connections.
out	Filters the outgoing connections.

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example uses ACL 20 to filter the incoming connections in line VTY 0 5.

```
FS(config)# line vty 0 5
FS(config-line)access-list 20 in
```

The following example uses the ACL named “test” to filter the outgoing connections in line VTY 6 7.

```
FS(config)# line vty 6 7
FS(config-line)access-list test out
```

Related Commands

Command	Description
show running	Displays status information

Platform Description N/A

3.2 accounting commands

Use this command to enable command accounting in the line. Use the **no** form of this command to restore the default setting.

accounting commands *level* { **default** | *list-name* }

no accounting commands *level*

Parameter Description

Parameter	Description
level	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
default	Default authorization list name.
list-name	Optional list name.

Defaults This function is disabled by default.

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA command accounting first, and then apply it on the line.

Configuration Examples The following example enables command accounting in line VTY 1 and sets the command level to 15.

```
FS(config)# aaa new-model
FS(config)# aaa accounting commands 15 default start-stop group tacacs+
FS(config)# line vty 1
FS(config-line)# accounting commands 15 default
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.3 accounting exec

Use this command to enable user access accounting in the line. Use the **no** form of this command to restore the default setting.

accounting exec { **default** | *list-name* }

no accounting exec

Parameter Description

Parameter	Description
default	Default authorization list name.
list-name	Optional list name.

Defaults This function is disabled by default.

Command Mode

Line configuration mode

Usage Guide

This function is used together with AAA authorization. Configure AAA EXEC accounting first, and then apply it on the line.

Configuration Examples

The following example enables user access accounting in line VTY 1.

```
FS(config)# aaa new-model
FS(config)# aaa accounting exec default start-stop group radius
FS(config)# line vty 1
FS(config-line)# accounting exec default
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.4 authorization commands

Use this command to enable authorization on commands, Use the **no** form of this command to restore the default setting.

authorization commands *level* { **default** | *list-name* }

no authorization commands *level*

Parameter Description

Parameter	Description
level	Command level ranging from 0 to 15. The command of this level is executed after authorization is performed.
default	Default authorization list name,
list-name	Optional list name.

Defaults

This function is disabled by default.

Command Mode

Line configuration mode

Usage Guide

This function is used together with AAA authorization. Configure AAA authorization first, and then apply it on the line.

Configuration Examples

The following example enables authorization on commands of level 15 in line VTY 1.

```
FS(config)# aaa new-model
FS(config)# aaa authorization commands 15 default group tacacs+
FS(config)# line vty 1
FS(config-line)# authorization commands 15 default
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.5 authorization exec

Use this command to enable EXEC authorization for the line. Use the **no** form of this command to restore the default setting.

authorization { **default** | *list-name* }

no authorization exec

Parameter Description

Parameter	Description
default	Default authorization list name,
list-name	Optional list name.

Defaults This function is disabled by default,

Command Mode Line configuration mode

Usage Guide This function is used together with AAA authorization. Configure AAA EXEC authorization first, and then apply it on the line.

Configuration Examples The following example performs EXEC authorization to line VTY 1.

```
FS(config)# aaa new-model
FS(config)# aaa authorization exec default group radius
FS(config)# line vty 1
FS(config-line)# authorization exec default
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 clear line

Use this command to clear connection status of the line.

clear line { **console** *line-num* | **vty** *line-num* **|** *line-num* }

Parameter Description

Parameter	Description
console	Clears connection status of the console line.
vty	Clears connection status of the virtual terminal line.
line-num	Specifies the line to be cleared.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear connection status of the line and restore the line to the unoccupied status to create new connections.

Configuration Examples

The following example clears connection status of line VTY 13. The connected session on the client (such as Telnet and SSH) in the line is disconnected immediately.

```
FS# clear line vty 13
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.7 disconnect-character

Use this command to set the hot key that disconnects the terminal service connection. Use the **no** form of this command to restore the default setting.

disconnect-character *ascii-value*

no disconnect-character

Parameter Description

Parameter	Description
ascii-value	ASCII decimal value of the hot key that disconnects the terminal service connection, in the range from 0 to 255.

Defaults

The default hot key is **Ctrl+D** and the ASCII decimal value is 0x04.

Command Mode Line configuration mode

Usage Guide This command is used to set the hot key that disconnects the terminal service connection. The hot key cannot be the commonly used ASCII node such as characters ranging from a to z, from A to Z or numbers ranging from 0 to 9. Otherwise, the terminal service cannot operate properly.

Configuration Examples The following example sets the hot key that disconnects the terminal service connection on line VTY 0 5 to **Ctrl+E** (0x05).

```
FS(config)# line vty 0 5
FS(config-line)# disconnect-character 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.8 escape-character

Use this command to set the escape character for the line. Use the **no** form of this command to restore the default setting.

escape-character *escape-value*

no escape-character

Parameter Description

Parameter	Description
escape-value	Sets the ASCII value corresponding to the escape character for the line, in the range from 0 to 255.

Defaults The default escape character is **Ctrl+^** (**Ctrl+Shift+6**) and the ASCII decimal value is 30.

Command Mode Line configuration mode

Usage Guide After configuring this command, press the key combination of the escape character and then press **x**, the current session is disconnected to return to the original session.

Configuration Examples The following example sets the escape character for the line to 23 (**Ctrl+w**).

```
FS(config)# line vty 0
FS(config-line)# escape-character 23
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

3.9 exec

Use this command to enable the line to enter the command line interface. Use the **no** form of this command to disable the function.

exec

no exec

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Line configuration mode

Usage Guide The **no exec** command is used to ban the line from entering the command line interface. You have to enter the command line interface through other lines,

Configuration Examples The following example bans line VTY 1 from entering the command line interface.

```
FS(config)# line vty 1
FS(config-line)# no exec
FS# show users
Line             User         Host(s)              Idle         Location
---------------- ------------ -------------------- ---------- ------------------
*   0 con 0      ---          idle                 00:00:00     ---
    1 vty 0      ---          idle                 00:01:03     20.1.1.2
    3 vty 2      ---          idle                 00:00:13     20.1.1.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.10 history

Use this command to enable command history for the line or set the number of commands in the command history. Use the **no history** command to disable command history. Use the **no history size** command to restore the number of commands in the command history to the default setting.

history [**size** *size*]

no history

no history size

Parameter Description

Parameter	Description
size *size*	The number of commands, in the range from 0 to 256.

Defaults This function is enabled by default, The default *size* is 10.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the number of commands in the command history to 20 for line VTY 0 5.

```
FS(config)# line vty 0 5
FS(config-line)# history size 20
```

The following example disables the command history for line VTY 0 5.

```
FS(config)# line vty 0 5
FS(config-line)# no history
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.11 length

Use this command to set the screen length for the line. Use the **no** form of this command to restore the default setting.

length *screen-length*

no length

Parameter Description

Parameter	Description
screen-length	Sets the screen length, in the range from 0 to 512.

Defaults The default is 24.

Command Mode

Line configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the screen length to 10.

```
FS(config-line)# length 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.12 line

Use this command to enter the specified LINE mode.

line [**console** | **vty**] *first-line* [*last-line*]

Parameter Description

Parameter	Description
console	Console port
vty	Virtual terminal line, applicable for telnet/ssh connection.
first-line	Number of first-line to enter

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to enter the specified LINE mode.

Configuration Examples

The following example enters the LINE mode from LINE VTY 1 to 3:

```
FS(config)# line vty 1 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.13 line vty

Use this command to increase the number of VTY connections currently available. Use the **no** form of this command to restore the default setting.

line vty *line-number*

no line vty *line-number*

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, there are five available VTY connections, numbered 0 to 4.

Command Mode Global configuration mode.

Usage Guide When you need to increase or decrease the number of available VTY connections, use the above commands.

Configuration Examples The following example increases the number of available VTY connections to 20. The available VTY connections are numbered 0 to 19.

```
FS(config)# line vty 19
Decrease the number of available VTY connections to 10. The available VTY connections are numbered 0-9.
FS(config)# line vty 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.14 location

Use this command to configure the line location description. Use the **no** form of this command to restore the default setting.

location *location*

no location

Parameter Description

Parameter	Description
location	Line location description

Defaults N/A

Command Mode

Line configuration mode

Usage Guide

N/A

Configuration Examples

The following example describes the line location as Swtich's Line VTY 0.

```
FS(config)# line vty 0
FS(config-line)# location Swtich's Line Vty 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.15 monitor

Use this command to enable log display on the terminal. Use the **no** form of this command to restore the default setting,

monitor

no monitor

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Line configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables log display on the terminal in VTY line 0 5.

```
FS(config)# line vty 0 5
FS(config-line)# monitor
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.16 privilege level

Use this command to set the privilege level for the line. Use the **no** form of this command to restore the default setting.

privilege level *level*

no privilege level

Parameter Description

Parameter	Description
level	Privilege level, in the range from 0 to 15.

Defaults The default is 1.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the privilege level for the line VTY 0 4 to 14.

```
FS(config)# line vty 0 4
FS(config-line)privilege level 14
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.17 refuse-message

Use this command to set the login refusal message for the line. Use the **no** form of this command to restore the default setting.

refuse-message [*c message c*]

no refuse-message

Parameter Description

Parameter	Description
c	Delimiter of the login refusal message, which is not allowed within the message.
message	Login refusal message.

Defaults N/A

Command Mode

Line configuration mode

Usage Guide

This command is used to set the login refusal message for the line. The characters entered after the ending delimiter are discarded directly, The login refusal message is displayed when the user has been refused to login.

Configuration Examples

The following example sets the login refusal message for the line to "Unauthorized user cannot login to the FS device".

```
FS(config-line)#vacant-message @ Unauthorized user cannot login to the FS device @
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.18 show history

Use this command to display the command history of the line.

show history

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the command history of the line.

```
FS# show history
exec:
sh privilege
sh run
show user
sh user all
show history
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

3.19 show line

Use this command to display line configuration.

show line { **console** *line-num* | **vty** *line-num* | *line-num* }

Parameter Description

Parameter	Description
console	Displays configuration for the console line.
vty	Displays configuration for the virtual terminal line.
line-num	Displays the line.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays configuration for the console port.

```
FS# show line console 0
CON      Type     speed    Overruns
* 0      CON      9600     45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 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: 53564 bytes
Total output:    395756 bytes
Data overflow:    27697 bytes
stop rx interrupt:    0 times
```

Field	Description
CON	Terminal type. CON indicates console; 0 indicates terminal line number and * ahead of the number means that the terminal is in use.
Type	Terminal type, including CON, and VTY.
speed	Asynchronous speed.
Overruns	The number of overrun errors received by the flash.

Line 0	Terminal line number.
Location: ""	Line location configuration.
Type: "vt100"	Compatibility standard.
Special Chars	Special characters, including Escape, Disconnect, and Activation characters.
Timeouts	Timeout value; “never” indicates no timeout.
History	Whether to enable command history; the number of commands in the command history.
Total input	Data volume received from the drive.
Total output	Date volume sent to the drive.
Data overflow	Overflowing data volume.
stop rx interrupt	Data reception interruption times.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.20 show privilege

Use this command to display the privilege level of the line.

show privilege

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the privilege level of the line.

```
FS# show privilege
Current privilege level is 10
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

3.21 show users

Use this command to display the login user information.

show users [**all**]

Parameter Description

Parameter	Description
all	Displays line user information, including users logging into the line and users not logging into the line.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about users logging into the line,

```
FS# show users
Line                User          Host(s)              Idle        Location
---------------- ------------ -------------------- ---------- ------------------
   0 con 0          ---           idle                 00:00:46    ---
   1 vty 0          ---           idle                 00:00:29    20.1.1.2
*  2 vty 1          ---           idle                 00:00:00    20.1.1.2
```

The following example displays all line user information,

```
FS(config)# show users all
Line                User          Host(s)              Idle        Location
---------------- ------------ -------------------- ---------- ------------------
   0 con 0          ---           idle                 00:00:49    ---
   1 vty 0          ---           idle                 00:00:32    20.1.1.2
*  2 vty 1          ---           idle                 00:00:00    20.1.1.2
   3 vty 2          ---                                00:00:00    ---
   4 vty 3          ---                                00:00:00    ---
   5 vty 4          ---                                00:00:00    ---
   6 vty 5          ---                                00:00:00    ---
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.22 speed

Use this command to configure the baud rate for the specified line. Use the **no** form of this command to restore the default setting,

speed *baudrate*

no speed

Parameter Description

Parameter	Description
baudrate	Sets the baud rate, in the range from 9600 to 115200.

Defaults The default is 9600.

Command Mode LINE configuration mode

Usage Guide N/A

Configuration Examples The following example sets the baud rate to 115200,

```
FS(config-line)# speed 115200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.23 terminal escape-character

Use this command to set the escape character for the current terminal. Use the **no** form of this command to restore the default setting.

terminal escape-character *escape-value*

terminal no escape-character

Parameter Description

Parameter	Description
escape-value	Sets the ASCII value corresponding to the escape character for the current terminal, in the range from 0 to 255.

Defaults The default escape character is **Ctrl+^** (**Ctrl+Shift+6**) and the ASCII decimal value is 30.

Command Mode Privileged EXEC mode

Usage Guide After configuring this command, press the key combination of the escape character and then press **x**, the current session is disconnected to return to the original session.

Configuration Examples The following example sets the escape character for the current terminal to 23 (**Ctrl+w**).

```
FS# terminal escape-character 23
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.24 terminal history

Use this command to enable command history for the current terminal or set the number of commands in the command history. Use the **no history** command to disable command history. Use the **no history size** command to restore the number of commands in the command history to the default setting.

terminal history [**size** *size*]

terminal no history

terminal no history size

Parameter Description

Parameter	Description
size *size*	Sets the number of commands, in the range from 0 to 256.

Defaults This function is enabled by default, The default *size* is 10.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the number of commands in the command history to 20 for the current terminal.

```
FS# terminal history size 20
```

The following example disables the command history for the current terminal.

```
FS# terminal no history
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

3.25 terminal length

Use this command to set the screen length for the current terminal. Use the **no** form of this command to restore the default setting.

terminal length *screen-length*

terminal no length

Parameter Description

Parameter	Description
screen-length	Sets the screen length, in the range from 0 to 512.

Defaults The default is 24.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the screen length for the current terminal to 10.

```
FS# terminal length 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.26 terminal location

Use this command to configure location description for the current device. Use the **no** form of this command to restore the default setting.

terminal location *location*

terminal no location

Parameter Description

Parameter	Description
location	Configures location description of the current device.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures location description of the current device as “Swtich’s Line Vty 0”.

```
FS# terminal location Swtich’s Line Vty 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.27 terminal speed

Use this command to configure the baud rate for the current terminal. Use the **no** form of this command to restore the default setting,

terminal speed *baudrate*

terminal no speed

Parameter Description

Parameter	Description
baudrate	Sets the baud rate, in the range from 9600 to 115200.

Defaults The default is 9600.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the baud rate for the current terminal to 115200,

```
FS# terminal speed 115200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.28 terminal width

Use this command to set the screen width for the terminal.

terminal width *screen-width*

terminal no width

Parameter Description

Parameter	Description
screen-width	Sets the screen width for the terminal, in the range from 0 to 256.

Defaults The default is 79.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the screen width for the terminal to 10.

```
FS# terminal width 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.29 timeout login

Use this command to set the login authentication timeout for the line. Use the **no** form of this command to restore the default setting.

timeout login response *seconds*

no timeout login response

Parameter Description

Parameter	Description
response	The time period during which the line waits for the user to enter any message.
seconds	Timeout value, in the range from 1 to 300 in the unit of seconds.

Defaults The default is 30.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example sets the login authentication timeout to 300 seconds for line VTY 0 5.

```
FS(config)# line vty 0 5
FS(config-line)login timeout response 300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.30 transport input

Use this command to set the specified protocol under Line that can be used for communication. Use the **no** form of this command to restore the default setting.

transport input { **all** | **ssh** | **telnet | none** }

no transport input { **all** | **ssh** | **telnet** | **none** }

Parameter Description

Parameter	Description
all	Allows all the protocols under Line to be used for communication
ssh	Allows only the SSH protocol under Line to be used for communication
telnet	Allows only the Telnet protocol under Line to be used for communication
none	Allows none of protocols under Line to be used for communication

Defaults **all**, **ssh** and **telnet** protocols are allowed.

Command Mode Line configuration mode

Usage Guide N/A

Configuration Examples The following example specifies that only the Telnet protocol is allowed to login in line vty 0 4.

```
FS(config)# line vty 0 5
FS(config-line)transport input ssh
```

Related Commands

Command	Description
show running	Displays status information

Platform Description N/A

3.31 vacant-message

Use this command to set the logout message. Use the **no** form of this command to restore the default setting.

vacant-message [*c message c*]

no vacant-message

Parameter Description

Parameter	Description
c	Delimiter of the logout message, which is not allowed within the message.
message	Logout message.

Defaults N/A

Command Mode Line configuration mode

Usage Guide This command is used to set the logout message for the line. The characters entered after the ending delimiter are discarded directly, The logout message is displayed when the user logs out.

Configuration Examples The following example sets the logout message to “Logout from the FS device”.

```
FS(config-line)#vacant-message @ Logout from the FS device @
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.32 width

Use this command to set the screen width for the line. Use the **no** form of this command to restore the default setting,

width *screen-width*

no width

Parameter Description

Parameter	Description
screen-width	Sets the screen width for the line, in the range from 0 to 256,

Defaults The default is 79.

Command Mode Line configuration mode

Usage Guide N/A

Configuration The following example sets the screen width for the line to 10.

Examples

```
FS(config-line)# width 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4 Password Policy Commands

4.1 password policy life-cycle

Use this command to set the password lifecycle. Use the **no** form of this command to restore the default setting.

password policy life-cycle days

no password policy life-cycle

Parameter Description

Parameter	Description
days	Sets the password lifecycle, in the range from 1 to 65535 in the unit of days.

Defaults No password lifecycle is set by default.

Command Mode Global configuration mode

Usage Guide This command is used to set the password lifecycle. After the password lifecycle expires, the system reminds you to change the password when you login next time.

ⓘ This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username *name* password *password* command) while not valid for the password in line mode.

Configuration Examples The following example sets the password lifecycle to 90 days.

```
FS(config)# password policy life-cycle 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.2 password policy min-size

Use this command to set the minimum length of the password. Use the **no** form of this command to restore the default setting.

password policy min-size *length*

no password policy min-size

Parameter Description

Parameter	Description
length	Sets the minimum length of the password, in the range from 1 to 31.

Defaults No minimum length of the password is set by default.

Command Mode Privileged EXEC mode

Usage Guide This command is used to set the minimum length of the password,

This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username *name* password *password* command) while not valid for the password in line mode.

Configuration Examples The following example sets the minimum length of the password to 8.

```
FS(config)# password policy min-size 8
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.3 password policy no-repeat-times

Use this command to ban the use of passwords used in the past several times. Use the no form of this command to restore the default setting.

password policy no-repeat-times *times*

no password policy no-repeat-times

Parameter Description

Parameter	Description
times	The past several times when passwords are configured, in the range from 1 to 31.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this function is enabled, passwords used in the past several times are recorded. If the new password has been used, the alarm message is displayed and password configuration fails.

This command is used to set the maximum number of password entries. When the actual number of password entries exceeds the configured number, the new password overwrites the oldest password.

This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username *name* password *password* command) while not valid for the password in line mode.

Configuration Examples

The following example bans the use of passwords used in the past five times.

```
FS(config)# password policy no-repeat-times 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.4 password policy strong

Use this command to enable strong password check.

password policy strong

no password policy strong

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide If the following two kinds of passwords are set not matching the strength policy, the alarm message is displayed.

1. The password the same as the username.
2. The simple password containing only characters or numbers.

ℹ This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username *name* password *password* command) while not valid for the password in line mode.

Configuration Examples

The following example configures the strong password check.

```
FS(config)# password policy strong
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.5 service password-encryption

Use this command to encrypt a password. Use the **no** form of this command to restore default setting.

service password-encryption

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is disabled by default. Various passwords are displayed in plain text, unless they are encrypted. After you run the **service password-encryption** and **show running** or **write** command to save your configuration, the password changes into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.

Configuration Examples The following example encrypts the password:

```
FS(config)# service password-encryption
```

Related Commands

Command	Description
enable password	Sets passwords of different privileges.

Platform Description N/A

4.6 show password policy

Use this command to display the password security policy set by the user.

show password policy

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the password security policy set by the user.

Configuration Examples

The following example displays the password security policy set by the user.

```
FS#show password policy
Global password policy configurations:
 Password encryption:                    Enabled
 Password strong-check:                  Enabled
 Password min-size:                      Enabled (6 characters)
 Password life-cycle:                  Enabled (90 days)
 Password no-repeat-times:               Enabled (max history record: 5)
```

Field	Description
Password encryption	Whether to encrypt the password.
Password strong-check	Whether to enable password strong-check.
Password min-size	Whether to set the minimum length of the password.
Password life-cycle	Whether to set the password lifecycle.
Password no-repeat-times	

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5 File System Commands

5.1 cd

Use this command to set the present directory for the file system.

cd *[filesystem:] [directory]*

Parameter Description

Parameter	Description
filesystem:	The URL of filesystem, followed by a colon (:). The filesystem includes **flash:**, **sata:**, **usb:** and **tmp:**.
directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults

The default directory is the flash root directory.

Command Mode

Privileged EXEC mode.

The specified path of the file system support URLs. For details of URL prefixes, see description of the **copy** command.

Usage Guide

Change the above parameter to the directory you want to enter. Use the **pwd** command to view the present directory.

Configuration Examples

The following example enters the sata hardware.

```
FS#pwd
flash:/
FS#cd sata:
FS#pwd
sata:/
```

Related Commands

Command	Description
pwd	Displays the present word directory.

Platform Description

N/A.

5.2 copy

Use this command to copy a file from the specified source directory to the specified destination directory.

copy *source-url destination-url*

Parameter Description

Parameter	Description
source-url	Source file URL, which can be local or remote.
destination-url	Destination file URL, which can be local or remote.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide when the file to be copied exists on the target URL, the target file system determines the action, such as error report, overwrite, or offering you the choice.

The following table lists the URL:

Prefix	Description
running-config	Running configuration file.
startup-config	startup configuration file.
flash:	local FLASH file system.
tftp:	The URL of TFTP network server, in the format as follows: **tftp**:[[//location]/directory]/**filename**

Configuration Examples The following example copies the netconfig file from device 192.168.64.2 to the FLASH disk and the netconfile file exists locally.

```
 FS#copy tftp://192.168.64.2/netconfig flash:/netconfig
Do you want to overwrite [/data/netconfig]? [Y/N]:y
Press Ctrl+C to quit
!
Copy success.
```

Related Commands

Command	Description
delete	Deletes the file.
rename	Renames the file.
dir	Displays the file list of the specified directory.

Platform Description N/A

5.3 delete

Use this command to delete the files in the present directory.

delete [*filesystem*:] *file-url*

Parameter Description

Parameter	Description
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, and **tmp:**.
file-url	The file name containing the path. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

Defaults

The default *filesystem*: is **flash:**.

Command Mode

Privileged EXEC mode.

Usage Guide

This command is used to delete the specified file in the URL. This command supports deleting the files stores in the local storage media, i.e., the URL must be one of the flash:/ usb0:/ or usb1:/ slave:/. If the prefix is not specified in the URL, it indicates to delete the file in the system.

In VSU mode, URLs do not support sw1-m1-disk0:/ series. For details of the supported prefixes, see the description of the **copy** command.

This command does not support wildcard.

Configuration Examples

The following example deletes the fstab file on the FLASH disk.

```
FS#pwd
flash:/
FS#dir
Directory of flash:/
1    -rw-          336    Jan 03 2012 18:53:42   fstab
2    -rw-         4096    Jan 03 2012 12:32:09   rc.d
3    -rw-     10485760    Jan 03 2012 18:13:37   rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
FS#delete flash:/fstab
Do you want to delete [flash:/fstab]? [Y/N]:y
Delete success.
FS#dir
Directory of flash:/
1    -rw-         4096    Jan 03 2012 12:32:09   rc.d
2    -rw-     10485760    Jan 03 2012 18:13:37   rpmdb
2 files, 0 directories
10,489,856 bytes total (13,192,992 bytes free)
```

Related Commands

Command	Description
copy	Copies the file.
dir	Displays the file list of the specified directory.

Platform Description

N/A

5.4 dir

Use this command to display the files in the present directory.

dir [*filesystem*:] [*directory*]

Parameter Description

Parameter	Description
filesystem	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, and **tmp:**.
directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults

By default, only the information under the present working path is displayed.

Command Mode

Privileged EXEC mode.

Usage Guide

Enter the specified directory to show the information of all the files in that directory. If no parameter is specified, the information of the files in the present directory is shown by default.

This command does not support wildcard.

Configuration Examples

The following example displays the file information of the root directory in the FLASH disk.

```
FS#dir flash:/
Directory of flash:/
1    -rw-          336    Jan 03 2012 18:53:42    fstab
2    -rw-         4096    Jan 03 2012 12:32:09    rc.d
3    -rw-     10485760    Jan 03 2012 18:13:37    rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

Field	Description
1, 2, 3…	Index number
-rw-	Permissions on a file include: ● d: directory ● r: read ● w: write ● x: executable
10485760	File size
rpmdb	File name
files	File number
directories	Directory number
total	Total size
free	Available space

Related Commands

Command	Description
pwd	Displays the present directory.

cd	Sets the present directory of the file system.

Platform Description

N/A.

5.5 erase

Use this command to erase the device or file that does't have a file system.

erase *filesystem*

Parameter Description

Parameter	Description
filesystem:	Name of the file system, followed by a colon (:). For example, usb0:.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example erases the USB filesystem.

```
FS#erase usb0:
Sure to erase usb0:? [Y/N] y
Erasing disk usb0 …
Erase disk usb0 done!
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.6 file

Use this command to display the information about a file.

file [*filesystem*:] *file-url*

Parameter Description

Parameter	Description
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, and **tmp:**.
file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults

The default *filesystem*: is **flash:**.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the information about gcc executable file.

```
FS#file flash:/gcc
/usr/bin/gcc-4.6: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.15, stripped
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.7 file prompt

Use this command to set the prompt mode.

file prompt [**noisy** | **quiet**]

Parameter Description

Parameter	Description
noisy	Displays prompt for all operation.
quiet	Displays prompt rarely.

Defaults

The default mode is noisy.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example sets the prompt mode to noisy.

```
FS#file prompt noisy
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.8 mkdir

Use this command to create a directory.

mkdir [*filesystem*:] *directory*

Parameter Description

Parameter	Description
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, and **tmp:**.
directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults

The default *filesystem*: is **flash**:.

The default *directory* is the root directory.

Command Mode

Privileged EXEC mode.

Usage Guide

Configuration Examples

The following example creates a directory named newdir:

```
FS#dir
Directory of flash:/
1    -rw-         336    Jan 03 2012 18:53:42   fstab
2    -rw-        4096    Jan 03 2012 12:32:09   rc.d
3    -rw-    10485760    Jan 03 2012 18:13:37   rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
FS#mkdir newdir
Created dir flash:/newdir
FS#dir
Directory of flash:/
1    -rw-         336    Jan 03 2012 18:53:42   fstab
2    -rw-        4096    Jan 03 2012 12:32:09   rc.d
3    -rw-    10485760    Jan 03 2012 18:13:37   rpmdb
4    drw-        4096    Jan 03 2012 18:13:37   newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
```

Related Commands

Command	Description
rmdir	Deletes the directory.
pwd	Displays the present directory.

Platform Description

N/A

5.9 more

Use this command to display the content of a file.

more [/**ascii** | /**binary**] [*filesystem*:] *file-url*

Parameter Description

Parameter	Description
/**ascii**	Displays the file content in the ASCII format.
/**binary**	Displays the file content in the
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, and **tmp:**.
file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults

The file is displayed in its own format by default.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the content of the netconfig file under root directory of FLASH disk.

```
FS#more flash:/netconfig
#
# The network configuration file. This file is currently only used in
# conjunction with the TI-RPC code in the libtirpc library.
#
# Entries consist of:
#
#       <network_id> <semantics> <flags> <protofamily> <protoname> \
#               <device> <nametoaddr_libs>
#
# The <device> and <nametoaddr_libs> fields are always empty in this
# implementation.
#
udp        tpi_clts      v     inet     udp     -       -
tcp        tpi_cots_ord  v     inet     tcp     -       -
udp6       tpi_clts      v     inet6    udp     -       -
tcp6       tpi_cots_ord  v     inet6    tcp     -       -
rawip      tpi_raw       -     inet     -       -       -
local      tpi_cots_ord  -     loopback -       -       -
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.10 pwd

Use this command to display the working path.

pwd

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults N/A.

Usage Guide This command displays the present working path

Configuration Examples The following example displays the process of switching the working directory from flash: to sata:.

```
FS#pwd
flash:/
FS#cd sata:/
FS#pwd
sata:/
```

Related Commands

Command	Description
cd	Changes the file system in the present directory.

Platform Description N/A.

5.11 rename

Use this command to move or rename the specified file.

rename src-url dst-url

Parameter Description

Parameter	Description
src-url	The source file URL to move.
dst-url	The URL of the destination file or directory.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

The following example renames the fstab file in the root directory on the FLASH disk as new-fstab.

```
FS#dir
Directory of flash:/
1    -rw-         336    Jan 03 2012 18:53:42    fstab
2    -rw-        4096    Jan 03 2012 12:32:09    rc.d
3    -rw-    10485760    Jan 03 2012 18:13:37    rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
FS#rename flash:/fstab flash:/new-fstab
Renamed file flash:/new-fstab
FS#dir
Directory of flash:/
1    -rw-         336    Jan 03 2012 18:53:42    new-fstab
2    -rw-        4096    Jan 03 2012 12:32:09    rc.d
3    -rw-    10485760    Jan 03 2012 18:13:37    rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

Related Commands

Command	Description
delete	Deletes the file.
copy	Copies the file.

Platform Description

N/A

5.12 rmdir

Use this command to delete an empty directory.

rmdir [*filesystem*:] *directory*

Parameter Description

Parameter	Description
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, and **tmp:**.
directory	

Defaults

The default *filesystem*: is **flash:**.

Command Mode

Privileged EXEC mode.

Usage Guide

This command does not support the wildcards, and the directory to be deleted must be empty. Since this command supports abbreviations, you can also use the **rm** command to delete empty directories.

Configuration

The following example deletes the null test directories.

Examples

```
FS#mkdir newdir
FS#dir
Directory of flash:/
1      -rw-              336      Jan 03 2012 18:53:42    fstab
2      -rw-             4096      Jan 03 2012 12:32:09    rc.d
3      -rw-       10485760      Jan 03 2012 18:13:37    rpmdb
4      drw-             4096      Jan 03 2012 18:13:37    newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
FS#rmdir newdir
removed dir flash:/newdir
FS#dir
Directory of flash:/
1      -rw-              336      Jan 03 2012 18:53:42    fstab
2      -rw-             4096      Jan 03 2012 12:32:09    rc.d
3      -rw-       10485760      Jan 03 2012 18:13:37    rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
```

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

5.13 show disk

Use this command to display sata/USB/Flash information.

show disk usb/**flash**

Parameter Description

Parameter	Description
usb	Displays USB information.
flash	Displays FLASH information.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays USB information.

```
FS#show disk usb
```

```
Disk /dev/sdb: 8159 MB, 8159477760 bytes
252 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 15624 * 512 = 7999488 bytes
```

The following example displays FLASH information.

```
FS#show disk flash
Nand flash size: 512MB
Nor flash size: 1MB
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.14 show file systems

Use this command to display the file system information.

show file systems

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to display the file systems supported in the present devices and the available space condition in the file system.

Configuration Examples

The following example displays the file system information:

```
FS#show file systems
  Size(KB)        Free(KB)      Type     Flags   Prefixes
        NA               NA          ram        rw    tmp:
        NA               NA     network       rw    tftp:
        NA               NA     network       rw    oob_tftp:
        NA               NA      xmodem        rw    xmodem:
      8192             2416         disk       rw    flash:
 167772160        147772160         disk       rw    sata0:
   1048576           548576         disk       rw    usb0:
```

Field	Description
Size(KB)	File system space, in the unit of KB.
Free(KB)	Available file system space, in the unit of KB.

Type	File system type
Flags	Permissions on the file system include: ● ro: read-only ● wo: write-only ● rw: read and write
Prefixes	File system prefix

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

5.15 show mount

Use this command to display the mounted information.

show mount

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

N/A

Usage Guide

N/A

Configuration Examples

The following example displays the mounted information.

```
FS#show mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro,commit=0)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
fusectl on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
/dev/sda3 on /hao-share type ext3 (rw,commit=0)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,noexec,nosuid,nodev)
```

Field	Description

proc	Source address of mount.
on	-
/proc	Destination address of mount.
type	-
proc	Mount type.
(rw,noexec,nosuid,nodev)	Mount property.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.16 tftp-client source

Use this command to bind a source IP address or source interface with a TFTP client. Use the **no** or **default** form of this command to restore the default setting.

tftp-client source { **ip** *ip-address* | *interface* }

no tftp-client source { **ip** *ip-address* | *interface*}

default tftp-client source { **ip** *ip-address* | *interface* }

Parameter Description

Parameter	Description
ip-address	Specifies the IPv4 source address.
interface	Specifies the source interface

Defaults

No source interface or IP address is bound with the TFTP client by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example binds source IP address 192.168.23.236 with the TFTP client.

```
FS(config)# tftp-client source ip 192.168.23.236
```

The following example binds source interface gigabitEthernet 0/0 with the TFTP client.

```
FS(config)# tftp-client source gigabitEthernet 0/0
```

The following example removes the configuration.

```
FS(config)# no tftp-client source ip 192.168.23.236
```

The following example restores the default setting.

```
FS(config)# default tftp-client source ip 192.168.23.236
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.17 tree

Use this command to display the file tree of the current directory.

tree [*filesystem*:] [*directory*]

Parameter Description

Parameter	Description
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, and **tmp:**.
directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults

The default *filesystem*: is **flash:**.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the file tree of flash:/echo

```
FS#tree flash:/echo
+-- client_module
+-- client_userspace
+-- echo_cli.c
+-- echo_client.c
+-- echo_client.h
+-- echo_client.o
+-- echo_cli.o
+-- echo_flag.h
+-- echo.h
+-- echo.ko
+-- echo_server.h
+-- exec_set_echo.h
+-- exec_show_echo.h
+-- Makefile
+-- module
¦   +-- echo.ko
¦   +-- echo.mod.c
¦   +-- echo.mod.o
¦   +-- echo_module.c
¦   +-- echo_module.o
¦   +-- echo.o
¦  +-- echo_server.c
¦  +-- echo_server.o
¦  +-- echo_sysfs.c
¦  +-- echo_sysfs.h
¦  +-- echo_sysfs.o
¦  +-- Makefile
¦  +-- modules.order
¦  +-- Module.symvers
¦  +-- msg_fd.c
¦  +-- msg_fd.o
+-- readme
+-- server_module
+-- server_userspace
+-- sys_FSOS.ko
+-- user_space
    +-- echo_server.c
    +-- echo_server.o
    +-- Makefile
    +-- msg_fd.c
    +-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free)
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.18 verify

Use this command to compute, display and verify Message Digest 5 (MD5).

verify [**/md5** *md5-value*] *filesystem***:** [*file-url*]

Parameter Description

Parameter	Description
/md5	Computes and displays MD5.
md5-value	The file MD5, which is compared with the computed MD5.
filesystem:	The URL of file system, followed by a colon (:). The file system includes **flash:**, **sata:**, **usb:**, and **tmp:**.
file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

Defaults

The default *filesystem:* is **flash:**.

Command Mode

Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example computes MD5 of flash:/gcc.

```
FS#verify flash:/gcc
8b072de7db7affd8b2ef824e7e4d716c
```

The following example

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6 LICENSING Commands

6.1 license copy

Use this command to back up a license file.

license { **copy-all** | **copy-file** *filename* } { **flash: | usb0:** } [*target-filename*]

Parameter description

Parameter	Description
copy-all	Copies all permanent license files in the system.
copy-file	Copies the *filename* license file in the system. And ***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.
filename	The name of a license file already installed in the system or the name of a feature
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.
target-filename	Specifies the name of the license file.

Command Mode

Privileged EXEC mode

Default Level

4

Usage Guide

When you back up all license files in the system, a tar file is generated. This command does not require authorization.

Both one license file and all license files of a certain feature can be copied.

Configuration Examples

The following example backs up all license files in the system into file-fs-license-lics in a USB flash drive (there must be this path) 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 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.

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.

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.

Prompt Messages

There is not permanent license in the system for backup.

```
Copy failed, there's no permanent license in the system.
```

All license files in the system are successfully backed up.

```
Success to copy all permanent license.
```

The error message is displayed if no feature or license file is specified on the device.

```
Copy failed, there’s no such service or license installed in the system.
```

The error message is displayed if the specified license file is temporary.

```
Copy failed, the license is temporary.
```

The specified license file is backed up successfully.

```
Success to copy license vsd.lic.
```

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).

6.2 license grace-period

Use this command to set the time of issuing a warning before the validity period of a license file expires. Use the **no** or **default** form of this command to restore the default setting.

license grace-peroid *license days*

no license grace-peroid *filename*

default license grace-peroid *filename*

Parameter Description

Parameter	Description
filename	The 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

Default Level

4

Usage Guide

When the timeout interval of a license file is shorter than the friendly period, the friendly period warning is generated once a day; and the warning is generated once an hour one day before the license file expires. Friendly period warning is issued in log or SNMP TRAP form.

⚠ This command does not require authorization.

⚠ An evaluation license file needs to be configured with friendly period warning. A permanent license file does not need to be configured with friendly period warning.

Configuration Examples

Verification

Prompt Messages

The specified license file is not in the system.

```
There's no license abc in the system.
```

Common Errors

Specify a license file not in the system.

6.3 license install

Use this command to install a license file.

license install { **flash:** | **usb0:** } *filename*

Parameter Description

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.

Command Mode

Privileged EXEC mode

Default Level

4

Usage Guide

The name of the license file can be modified. This command does not require authorization.

Configuration Examples

Verification

Run the **show license all_license** command to check the license name. If the license name is displayed, the corresponding license file is installed.

Prompt Messages

The specified license file is not in the system.

```
Install failed: no such file or directory.
```

The specified license file is not legal.

```
Install failed: the install license may be wrong.
```

The specified license file is newer than the installed one.

```
Install failed: the system already has a same license which is newer.
```

The license file is reinstalled.

```
Install failed: the license has been installed before.
```

The specified license file is temporary and there is the same permanent one.

```
Install failed: The system already has a same permanent license.
```

Common Errors

Specify a license file not on the device.

Specify a license file illegal.

Specify a license file to install older than existing one in the system.

Reinstall the license file.

Replace the permanent license file with the temporary license file.

6.4 license unbind

Use this command to unbind a license.

license unbind *pak*

Parameter Description

Parameter	Description
pak	The license code

Command Mode

Privileged EXEC mode

Default Level

4

Usage Guide

This command does not require the license.

⚠ Use this command to unbind a license from the bound device before performing unbinding on the Web page.

⚠ You will get an authenticode after unbinding the license from the device, which is necessary for unbinding operation on the Web page.

Configuration

The following example unbinds license code LIC-FCOE00000012268888.

Examples

```
FS#license unbind LIC-FCOE00000012268888
Success to unbind license LIC-FCOE00000012268888.
The verification string is 775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355855.
```

6.5 license uninstall

Use this command to remove a license file.

license uninstall { **all** | *license* [*filename*] }

Parameter Description

Parameter	**Description**
all	Removes all license files in the system.
license	The name of the license to be removed
filename	The name of the file to be removed

Command Mode

Privileged EXEC mode

Default Level

4

Usage Guide

This command does not require authorization.

⚠ 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.

Configuration Examples

Verification

Run the **show license all_license** command to view the **Service name** filed. If the name of a feature corresponding to a license file already removed is not displayed, the removal is successful.

Prompt Messages

The specified license file is not on the device. (it is named after defd in this example).

```
Uninstall failed: there's no license defd in the system.
```

The specified license file of the specified feature is not on the device (The specified feature is LIC-WLAN-AP-32 and the specified license is named 123.lic).

```
Uninstall failed: there's no license 123.lic of service LIC-WLAN-AP-32 in the system.
```

The single instance license does not support license based uninstalling.

```
Uninstall failed: single instance license does not support license based uninstalling.
```

The removing of a license file is successful (LIC-WLAN-AP-32 is the name of the specified file and AP32_1.lic is a license file in this example).

```
Uninstall license AP32_1.lic of service LIC-WLAN-AP-32 success.
```

Common Errors

The license file has not been installed on the device.

Specify a license file not on the device.

Remove a certain license file for a single-instance feature (One single-instance license does not support the removing of one single file.

6.6 license update

Use this command to update a license file.

license update { **flash:** | **usb0:** } *filename*

Parameter Description

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.

Command Mode

Privileged EXEC mode

Default Level

4

Usage Guide

This command does not require authorization. The name of a license file can be modified.

Configuration Examples

Verification

Run the **show license** command to check the **Attribute** field. If the field is displayed as Permanent, the corresponding attribute is updated.

Configuration Examples

```
FS #show    license all-license
Searching license in the system...
  1. Service name: LIC-VSD
Attribute: Permanent, Multiple instance, Releasable
Installed licenses(s): 123.lic
```

Prompt Messages

The specified license file is not in the system.

```
Update failed: No such file or directory.
```

The specified license file is not legal.

```
Update failed: the update license may be wrong.
```

The specified license file is newer than the installed one.

```
Update failed: the new installed license is older than the system one.
```

The license file is reinstalled.

```
Update failed: the license has been installed before.
```

The temporary license file cannot be replaced by a permanent one.

```
Update failed: the period license cannot replace permanent license.
```

The specified license file is not on the device before the corresponding feature of the license file is to be installed first.

```
Update failed: now the system does not have the license.
Try "license install" instead.
```

Common Errors

Install a license file that does not belong to the present device.

Replace the license file of the new version with the old version.

Reinstall an updated license file.

Replace the permanent license file with the temporary license file.

Start update when the corresponding feature is not licensed for the system.

6.7 show license

Use this command to check a license file for the device.

show license { **all-license | dev-license | file** [*license*] }

Parameter Description

Parameter	Description
all-license	The list of all license files already installed on the device
dev-license	The list of the license files on all devices
file *filename*	The name of a specified license file

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

This command does not require authorization. It displays the license information of the system.

Configuration Examples

The following example displays the information of all the license files installed in the system.

```
FS#show    license all-license
Searching license in the system...
1. Service name: LIC-AP-64
    Attribute: Releasable
    [Permanent licenses]        [Licensed serial number]
    19880966.lic                  LIC-AP-6400000012264966
    19880988.lic                  LIC-AP-6400000012264988

    [Temporary license]         [Licensed serial number]
    19880900.lic                  LIC-AP-6400000012264900
    (63 days left)
```

The following example displays the information of the license files on all devices.

```
FS#show    license dev-license
Searching license in the system...
Dev:1
 1. Service name: LIC-AP-64
    Attribute: Releasable
    [Permanent licenses]        [Licensed serial number]
    19880966.lic                  LIC-AP-6400000012264966
    19880988.lic                  LIC-AP-6400000012264988

    [Temporary license]         [Licensed serial number]
    19880900.lic                  LIC-AP-6400000012264900
    (63 days left)

Dev:2
 1. Service name: LIC-FC-BLADE-S
    Attribute: Temporary, Releasable
    Left days: 99
    Licensed serial number: LIC-FC-BLADE-S 00000001884686
2. Service name: LIC-AP
    Attribute: Permanent, Releasable
    [Installed licenses]        [Licensed serial number]
    19880921.lic                  LIC-AP00000012265001
19880922.lic                  LIC-AP00000012265002

```

Field Description:

Field	Description
Service name	The name of the feature of the license file
Attribute	Some features of the license file
Left days	The remaining days of the expiry time of the license file

Installed license	Installed license file
Licensed serial number	License code

6.8 show license hostid

Use this command to display the host ID for the license (one device).

show license hostid

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require authorization. There is a unique serial number for identifying each device.

Configuration Examples

The following example displays the host ID for the license (one device).

```
FS#show license hostid
1234942570021
```

6.9 show license unbind-code

Use this command to display the unbound license code on the current device.

show license unbind-code

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command does not require license.

Configuration Examples

6.10 show license usage

Use this command to display the status of current license file in the system.

show license usage

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

This command does not require authorization.

Configuration Examples

The following example displays the status of current license file in the system.

```
FS#show license usage
Searching license in the system...
 1. Service name: LIC-AP-64
    Attribute: Releasable
    [Permanent licenses]     [Licensed serial number]
    19880966.lic               LIC-AP-6400000012264966
    19880988.lic               LIC-AP-6400000012264988

    [Temporary license]      [Licensed serial number]
    19880900.lic               LIC-AP-6400000012264900
    (63 days left)
```

Field Description

Field	Description
Service name	The feature name of the license file
Attribute	The attributes of the license file
Left days	The remaining days of the expiry time of the license file

7 PKG_MGMT Commands

7.1 clear storage

Use this command to remove an installation package on the local device.

clearstorage[*url*]

Parameter Description

Parameter	Description
url	A local *url* directory or full path name indicates where the installation package is stored

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide This command is used to remove an installation package or all packages in a directory and all installation packages on the local device.

Configuration Examples

```
FS#clear storage
Remove the whole storage directory?[y/n]y
FS#clear storage usb0
Remove the file or directory usb0 from the storage?[y/n]y
FS#
```

Verification Check specified *url*

Platforms N/A

7.2 patch active

Use this command to activate a patch to take effect.

patch active

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Default Level

2

Usage Guide

Activating operation can be performed only on the device already installed with a patch, after which the patch really takes effect. This command can be used to activate a hot patch temporarily. The activated patch becomes invalid after device restart.

Configuration Examples

The following example activates a patch on the box device.

```
FS#patch active
 Active the patch package success
```

The following example activates a patch on the chassis device.

```
FS#patch active slot 8
[Slot 8]:
 Active the patch package success
```

Verification

Use the **show patch** command to display patch information.

Prompt Messages

The patch is activated successfully.

```
Active the patch package success
```

The running fails and a patch package needs to be installed at first.

```
Patch not installed
```

There is no need to run the command for the patch in the activated or running status.

```
The patch status is already active or running
```

Contact the service center to solve the package problem.

```
Cannot find the package's scripts file
```

Common Errors

There is no hot patch installed on current device.

The hot patch on current device is already activated.

Platforms

N/A

7.3 patch deactive

Use this command to deactivate a patch.

patch deactive

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

This commandcan be performed to deactivate a patch only after the patch is in the activated status.

Configuration Examples

The following example deactivates a patch on the box device.

```
FS#patch deactive
 Deactive the patch package success
```

The following example deactivates a patch on the chassis device.

```
FS#patch deactive slot 8
 [Slot 8]:
Deactive the patch package success
```

Verification

Use the **show patch** command to display patch information.

Prompt Messages

The patch is deactivated successfully.

```
Deactive the patch package success
```

The running fails and a patch package needs to be installed at first.

```
Patch not installed
```

There is no need to run the command for the patch in the deactivated status.

```
The patch is not in active or running status
```

Contact the service center to solve the package problem.

```
Cannot find the package's scripts file
```

Common Errors

There is no hot patch installed on current device.

The hot patch on current device is already invalid.

7.4 patch delete

Use this command to uninstall a patch.

patch delete

Parameter Description

Parameter	Description
N/A	N/A

Command

Privileged EXEC mode

Mode

Default Level 2

Usage Guide This command is used to remove the existing hot patch package on the device.

Configuration Examples The following example removes the installed hot patch package from the box device.

```
FS# patch delete
Clear the patch patch_bridge success
Clear the patch success
```

The following example removes the installed hot patch package from the chassis device.

```
FS# patch delete slot M1
[Slot M1]:
Clear the patch patch_bridge success
Clear the patch success
```

Verification Use the **show patch** command to display patch status.

Prompt Messages The patch is uninstalled successfully.

```
Clear the patch success
```

A hot patch package should be installed at first for it has not been installed.

```
Patch not installed
```

Common Errors There is no hot patch installed on current device.

7.5 patch running

Use this command to activate a patch permanently.

patch running

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 2

Usage Guide Activating operation can be performed only on the device already installed with a patch, after which the patch really takes effect. This command can be used to activate a hot patch permanently.

Configuration Examples

The following example activates a patch on the box device.

```
FS#patch running
The patch on the system now is in running status
```

The following example activates a patch on the chassis device.

```
FS#patch running slot M1
[Slot M1]:
The patch on the system now is in running status
```

Verification

Use the **show patch** command to display the patch information.

Prompt Messages

The patch is activated permanently.

```
The patch on the system now is in running status
```

The running fails and a patch package needs to be installed at first.

```
Patch not installed
```

There is no need to run the command for the patch is in the deactivated status.

```
The patch is not in active or running status
```

Contact the service center to solve the package problem.

```
Cannot find the package's scripts file
```

Common Errors

There is no hot patch on current device.

The hot patch is already activated on current device.

7.6 show component

Use this command todisplay all components already installed on current device and their information.

show component [*component_name*]

Parameter Description

Parameter	Description
component_name	Name of the components 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 isintact, and check whether this component works properly.

Command

Privileged EXEC mode

Mode

Default Level 2

Usage Guide This command includes one with *component_name* and one without *component_name*. During upgrade, it requires users to understand all components installed on current device and their version information before components deletion. This needs to use the **show component** command without *component_name*. The **show component** command with *component_name* is used to obtain details of the corresponding component. The detailed information enables users to easily realize components' operation and damage. It is significant to insure their troubleshooting, security and reliability.

Some components in use will change their defaults files. Though this is more possibly normal than malicious, the **show component** command is used only to judge whether component files change in use. It is unable to distinguish natural damage from malicious one. It depends on users to make a further judgment.

Configuration Examples The following example displays all components already installed on the box device and their information.

```
FS# show component
Package      :sysmonit
        Version:1.0.1.23cd34aa          Build time: Wed Dec    7 00:58:56 2013
        Size:12877  Install time :Wed  Mar 5 14:23:12 2012
        Description: this is a system monit package
        Required packages: None
-------------------------------------------------------------------
Package:bridge
        Version:2.0.1.37cd5cda          Build time: Wed Dec    7 00:54:56 2013
        Size:23245  Install time :Wed  Mar 5 14:30:12 2012
        Description: this is a bridge package
        Required packages: None
-------------------------------------------------------------------
```

This command is used to obtain all components already installed on the device and theirbasic information. The information offers a basis for users to decide whether to upgrade or delete components.

Field	Description
Package	Name of the component
Version	Version number of the component
Build time	Compilation time of the component on the server
Size	Content size of the component
Install time	Installation time of the component
Description	Simple functional description of the component
Required packages	Name of required packages

The following example displays the information of all feature components already installed on the chassis device.

```
FS#show component slot 8
FS#*
```

```
[Slot 8]:
Package : utils-system
        Version: 1.0.0.433ef8d              Build time: Sun May 19 19:22:54 2013
        Size: 823936      Install time: Sun May 19 19:27:04 2013
        Description: utils system compile
        Required packages: None
-----------------------------------
Package : tcl-expect
        Version: 1.0.0.433ef8d              Build time: Sun May 19 19:19:18 2013
        Size: 3474153                 Install time: Sun May 19 19:27:04 2013
        Description: tcl & expect packages
        Required packages: None
-----------------------------------
```

The following example displays the information of specified components already installed on the box device.

```
FS# show componentbridge
package:bridge
        Version: 2.3.1.1252ea            Build time: Wed Dec    7 00:54:56 2013
        Size:26945   Install time : Wed Mar 19:23:15 2012
        Description:this is a bridge package
        Required packages: None
        Package files:
             /lib64
             /lib64/libbridge.so
             /sbin
        /sbin/bridge

      Package file validate: [OK]
      Required relationship verify: [OK]
```

The other information except the basic information of components is listed as follows.

Field	Description
Package file validate	Checks whether the component filesare intact. “OK” is displayed when all component files work properly; “ERR” is displayed together with their names when some component files are lost or revised.
Required package	Lists all required packages of the component. “OK” is labeled if required components are already installed; “ERR” is labeled if not together with detailed description about their names and versions.
Package files	Lists all files contained in the package.

Prompt Messages

The execution is successful with all components information displayed.

```
Package      :sysmonit
```

```
        Version:1.0.1.23cd34aa          Build time: Wed Dec     7 00:58:56 2013
        Size:12877  Install time :Wed  Mar 5 14:23:12 2012
        Description: this is a system monit package
        Required packages: None
--------------------------------------------------------------------
Package:bridge
        Version:2.0.1.37cd5cda          Build time: Wed Dec     7 00:54:56 2013
        Size:23245  Install time :Wed  Mar 5 14:30:12 2012
        Description: this is a bridge package
        Required packages: None
--------------------------------------------------------------------
```

7.7 show patch

Use this command to display the information of a hot patch package already installed on the device.

show patch[*patch _name*]

Parameter Description

Parameter	Description
patch _name	Name of the patches 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

Default Level

2

Usage Guide

This command is used to check all patches already installed on the device and their information.

Configuration Examples

The following example displays all patches already installed on the box device.

```
FS# show patch
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
```

This command is used to obtain the basic information of all patches already installed on the device.

Field	Description
Package	Name of the patch
status	Status of the patch
Version	Version of the patch
Build time	Compilation time of the patch on the server
Size	Content size of the patch
Install time	Installation time of the patch
Description	Simple functional description of the patch

The following example displays the information of all patches installed on the chassis device.

```
FS#show patch slot 8
[Slot 8]:
Patch package patch_install installed in the system, version:pa1
Package : patch_test
Status: running
      Version: 1.0.0.05151504
      Build time: Wed May 15 07:04:28 2013
      Size: 1804
      Install time: Thu Jan   1 00:56:43 1970
      Description: Experimentation
      Required packages: None
-----------------------------------
```

The following example displays the information of particular patches installed on the box device.

```
FS# show componentbridge
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
      Package files:
          /lib64
          /lib64/libbridge.so
          /sbin
      /sbin/bridge

     Package file validate: [OK]
```

The other information except the basic information of the patch is listed as follows:

Field	Description
Package file validate	Checks whether the patch files are intact. "OK" is displayed when all patch files work properly; "ERR" is displayed together with their names when some files are lost or revised.

Package files	Lists all files contained in the patch package.

Prompt Messages

The information of the patch is displayed after successful running.

```
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
```

7.8 show upgrade file

Use this command to display the information of the installation package files in the device file system.

show upgrade file *url*

Parameter Description

Parameter	Description
url	The local *url* path indicates where an installation package file is stored.

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

This command is used to preview main messages of an installation package after it is downloaded into local file system.

This command is not applied to a chassis package.

Configuration Examples

The following example displays the information of an installation package file.

```
FS# show upgrade file flash://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
Name          : bridge
Version:1.0.1.23cd34aa
Package type           : common component
Support target        : eg1000m
Size                         : 26945
Build time              : Wed Dec    7 00:54:56 2013
Install date           : (not installed)
Description             : this is a bridge package
Package files :
          Package files:
                /lib64
                /lib64/libbridge.so
                /sbin
          /sbin/bridge
```

This command is used to obtain the information in the package.

Field	Description
Name	Name of the package
Version	Version of the package
Package type	Type of the package
Support target	Supported product description
Size	Content size of the package
Build time	Compilation time of the package
Install date	Installation time of the package
Description	Description of the package
Package files	All contents in the package

Prompt Messages

The package information is displayed after running.

```
Name         : bridge
Version:1.0.1.23cd34aa
Package type          : common component
Support target       : eg1000m
Size                         : 26945
Build time              : Wed Dec    7 00:54:56 2013
Install date          : (not installed)
Description            : this is a bridge package
Package files :
      Package files:
          /lib64
          /lib64/libbridge.so
          /sbin
   /sbin/bridge
```

7.9 show upgrade history

Use this command to display the upgrade history.

show upgrade history

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

2

Configuration

The following example displays the upgrade history.

Examples

```
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
```

Prompt Messages

N/A

Platforms

N/A

7.10 upgrade

Use this command to install and upgrade an installation package in the local file system.

upgrade [*url* [**force**]

Parameter Description

Parameter	Description
url	The local path indicates where an installation package is stored. This command is used to upgrade an installation package on the device.
force	Mandatory upgrade

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

This command is applicable to installation packages of all subsystem components, chassis devices, feature components and hot patches. Before its use, run the **copy** command to copy feature packages into the file system in the device.

When there is no specified range of parameters, the command is used to upgrade the matched system components according to the auto-sync configuration.

Configuration Examples

The following example upgrades the main package on the device.

```
FS#upgrade usb0:/eg1000m_main_1.0.0.0f328e91.bin
Upgrade processing is 10%
Upgrade processing is 60%
Upgrade processing is 90%
Upgrade info [OK]
Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
Upgrade processing is 100%
```

```
Reload system to take effect!
```

The following example upgrades the chassis package on the device.

```
FS# upgrade usb0:/ S8600E_FSOS11.0(4)B1_CM_install.bin
[Slot M1]:Upgrade processing is 10%

 [Slot 1]:Upgrade processing is 10%

 [Slot M1]:Upgrade processing is 60%

 [Slot 1]:Upgrade processing is 60%

 [Slot M1]:Upgrade processing is 90%

 [Slot M1]:
 Upgrade info [OK]
     Kernel version[2.6.32.abb2b41f170c81->2.6.32.abb2b415749f40]
     Rootfs version[1.0.0.d5f0de03->1.0.0.660e0085]

 [Slot M1]:Restart to take effect !

 [Slot M1]:Upgrade processing is 100%
 [Slot 1]:Upgrade processing is 90%

 [Slot 1]:
 Upgrade info [OK]
     Kernel version[2.6.32.9f8b56f1d45ab2 ->2.6.32.0f48cb9f170c81]
     Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]

 [Slot 1]:Restart to take effect !

 [Slot 1]:Upgrade processing is 100%
 [slot: M1]
     device_name: ca-octeon-cm
     status:            SUCCESS
 [slot: 1]
     device_name: ca-octeon-lc
Status:            SUCCESS
```

Verification

Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.

Run the **show component** command to check whether the upgrade of a feature component is successful.

upgrading a feature component

Run the **show patch** command to check whether the upgrade of a hot patch is successful.

Prompt Messages

The prompt message of successful running is displayed.

```
Upgrade info [OK]
```

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade command.

```
Device don't support
```

There is no need to upgrade the device.

```
The version in device is newer or the same
```

When there is insufficient space for upgrade, check USB flash disk attached on the device.

```
No enough space for decompress
```

Contact the service center to solve the system problem.

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

The existing patch package needs to be uninstalled before upgrade.

```
Already exist patch, please uninstall before upgrade
```

The patch package is not applicable to this system and needs to be changed.

```
Patch compatibility err
```

The upgrade of a patch package is not available on this device and needs to be regained.

```
some origin cmpnt has change
```

7.11 upgrade auto

Use this command to upgrade an installation package 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.

upgrade auto *url* [**force**]

Parameter Description

Parameter	Description
url	Installation package directory
force	Enforces upgrade.

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

Use this command to upgrade the VSU system.

Download the program of the latest version to the device before running this command (by using the **copy tftp** command).

During one upgrade, do not use the **upgrade auto** command and other upgrade commands (such as the **upgrade** command) at the same time. If auto-upgrade fails, follow the system prompt to restore the version.

Do not update the installation package (by running the copy tftp command/U disk copy) or perform other upgrade operation (running the upgrade /upgrade auto command) repetitively.

During auto-upgrade, do not unplug the card, perform hot backup switchover, power off chassis or change VSU software/hardware configuration.

Configuration Examples

The following example upgrades the main package automatically without interrupting the service.

```
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.
```

7.12 upgrade download tftp

Use this command to download, install and upgrade installation packages from the tftp server.

upgrade download tftp:/*path* [**force**]

upgrade download oob_tftp:/*path* [**force**]

Parameter Description

Parameter	Description
path	The path of installation packages on the tftp server This command is downloaded and upgraded automatically from the server.
force	Enforces upgrade.

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

This command is applicable to installation packages of all subsystem components, chassis devices, feature components and hot patches. This command is used to perform automatic installation, copy and upgrade of files.

Configuration Examples

The following example upgrades the main package.

```
FS# upgrade download tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
  Upgrade processing is 10%
  Upgrade processing is 60%
  Upgrade processing is 90%
  Upgrade info [OK]
                Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
                Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
  Upgrade processing is 100%
Reload to take effect!
```

Verification

Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.

Run the **show component** command to check whether the upgrade of a feature component is successful.

Run the **show patch** command to check whether the upgrade is successful of a hot patch package.

Prompt Messages

The prompt message of successful running is displayed.

```
Upgrade info [OK];
```

The installation package is invalid or damaged and needs to be regained for upgrade command.

```
Invalid package file
```

The installation package is not available on the device and needs to be regained for upgrade command.

```
Device don't support
```

There is no need to upgrade the device.

```
The version in device is newer or the same
```

When there is insufficient space for upgrade, check USB flash disk attached on the device.

```
No enough space for decompress
```

Contact the service center to solve the system problem.

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

The existing patch package needs to be deleted.

```
Already exist patch, please uninstall before upgrade
```

The patch package is not compatible on this device. Replace the package..

```
Patch compatibility err
```

The upgrade of the patch package is not applied to the device. Regain the package.

```
Some origin component has change
```

7.13 upgrade rollback

Use this command to roll a subsystem back to the version before the upgrade.

upgrade rollback

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

2

Usage Guide

This command is used when the device cannot work properly after subsystem upgrade. It takes effect only when the last upgrade of subsystem components is successful.

The command is valid after device restart. The recursive rollback cannot be executed through this command in succession.

Configuration Examples

The following example rolls a subsystem back to the version before the upgrade on the box device.

```
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!
```

The following example rolls a subsystem back to the version before the upgrade on the chassis device.

```
FS#upgrade rollback slot M1
[Slot M1]:
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!
```

Verification

Run the **show version detail** command to check the result of rolling back subsystem components after device restart.

Prompt Messages

The prompt message of successful running is displayed.

```
Rollback success!
Restart to take effect !
```

The rollback operation cannot be performed when subsystem components have not been upgraded last time.

```
Not subsys package last upgrade
```

The rollback operation cannot be performed for the last upgrade is not successful.

```
Last upgrade err or skip
```

The upgrade command has not been run or the rollback operation has been performed.

```
Monitor file lost
```

Common Errors

The last upgrade is not for subsystem components, but for feature packages, hot patch packages and so on. Run the rollback command for subsystem once.

8 CWMP Commands

8.1 acs password

Use this command to configure the ACS password to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to cancel the configuration.

acs password { *password* | *encryption-type encrypted-password* }

no acs password

Parameter Description

Parameter	Description
password	Configures the ACS user password to be authenticated for the CPE to connect to the ACS.
encryption-type	Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used).
encrypted-password	Specifies the password in encrypted form.

Defaults

encryption-type: 0

encrypted-password: N/A

Command Mode

CWMP configuration mode

Usage Guide

Use this command to configure the ACS user password to be authenticated for the CPE to connect to the ACS. 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:

- ⓘ The command contains English letters in upper or lower case and numeric characters.
- ⓘ Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

Configuration Examples

The following example configures the ACS password to be authenticated for the CPE to connect to the ACS to 123.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#acs password 123
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

acs username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Platform Description N/A

8.2 acs url

Use this command to configure the URL of the ACS to which the CPE will connect.

Use the **no** form of this command to restore the default setting.

acs url *url*

no acs url

Parameter Description

Parameter	Description
url	Specifies the URL of the ACS.

Defaults N/A

Command Mode CWMP configuration mode

Usage Guide Use this command to configure the URL of the ACS to which the CPE will connect. If no ACS URL is manually specified but a dynamic ACS URL is obtained through DHCP, the CPE initiates a connection to the ACS using the dynamically obtained ACS URL. The URL of the ACS should meet the following format requirements:

- The URL of the ACS is formatted as http://host[:port]/path or https://host[:port]/path.
- The URL of the ACS consists of at most 256 characters.

Configuration Examples The following example specifies the URL of the ACS to http://10.10.10.1:8080/acs.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#acs url http://10.10.10.1:8080/acs
FS(config-cwmp)#
```

The following example specifies the URL of the ACS to http://www.test.com/service/tr069servlet.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#acs url http://www.test.com/service/tr069servlet
FS(config-cwmp)#
```

Related Commands

Command	Description

show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

8.3 acs username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to restore the default setting.

acs username *username*

no acs username

Parameter Description

Parameter	Description
username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Defaults N/A

Command Mode CWMP configuration mode

Usage Guide Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Configuration Examples The following example configures the ACS username to be authenticated for the CPE to connect to the ACS to admin.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#acs username admin
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs password	Configures the ACS password to be authenticated for the CPE to connect to the ACS.

Platform Description N/A

cpe back-up

Use this command to configure the backup and restoration of the main program and configuration file of the CPE.

Use the **no** form of this command to disable this function.

cpe back-up [**delay-time** *seconds*]

no cpe back-up

Parameter Description

Parameter	Description
seconds	Specifies the delay for backup and restoration of the main program and configuration file of the CPE, in the range from 30 to 10,000 in the unit of seconds

Defaults

The default is 60 seconds.

Command Mode

CWMP configuration mode

Usage Guide

You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its main program or configuration file. Then when the CPE fails to connect to the ACS and breaks away from the NMS after its main program or configuration file is upgraded, the previous main program or configuration file 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 main program or configuration file.

Configuration Examples

The following example disables the backup and restoration of the main program and configuration file of the CPE.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#no cpe back-up
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description

N/A

8.4 cpe back-up

Use this command to enable the CPE backup function.

Use the **no** form of this command to restore the default setting.

cpe back-up [**delay-time** *seconds*]

no cpe back-up

Parameter Description

Parameter	Description
seconds	Sets the backup delay time (30-10,000 seconds).

Defaults

The default is 60 seconds.

Command Mode

CWMP configuration mode

Usage Guide

After updrading main programs or configurations, CPE cannot communicate with ACS for wrong configuration delivery. Use this command to recover the previous programs and configurations.

Configuration Examples

The following example disables the CPE backup function.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#no cpe back-up
FS(config-cwmp)#
```

Platform Description

N/A

8.5 cpe inform

Use this command to configure the periodic notification function of the CPE.

Use the **no** form of this command to restore the default setting

cpe inform [**interval** *seconds*] [**starttime** *time*]

no cpe inform

Parameter Description

Parameter	Description
seconds	Specifies the periodical notification interval of the CPE in the range from 30 to 3,600 in the unit of seconds.
time	Specifies the date and time for starting periodical notification in yyyy-mm-ddThh:mm:ss format.

Defaults

The default is 600 seconds.

Command Mode

CWMP configuration mode

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.

The narrower periodical notification interval allows the ACS to track the latest CPE status more accurately. However, narrower periodical notification interval brings about more sessions between the CPE and the ACS, consuming more resources of them. So the user should specify the periodical notification interval of the CPE to a reasonable value according to the network performance and the ACS performance.

Configuration Examples

The following example specifies the periodical notification interval of the CPE to 60 seconds.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#cpe inform interval 60
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description

N/A

8.6 cpe password

Use this command to configure the CPE password to be authenticated for the ACS to connect to the CPE. Use the **no** form of this command to cancel the configuration.

cpe password { *password* | *encryption-type encrypted-password* }

no cpe password

Parameter Description

Parameter	Description
password	Configures the CPE user password to be authenticated for the ACS to connect to the CPE.
encryption-type	Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used).
encrypted-password	Specifies the password in encrypted form.

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:

- The command contains English letters in upper or lower case and numeric characters.
- Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

Configuration Examples

The following example configures the CPE password to be authenticated for the ACS to connect to the CPE to 123.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#cpe password 123
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Platform Description

N/A

8.7 cpe url

Use this command to configure the URL of the CPE to which the ACS will connect.

Use the **no** form of this command to restore default setting.

cpe url *url*

no cpe url

Parameter Description

Parameter	Description
url	Specifies the URL of the CPE.

Defaults

N/A

Command Mode

CWMP configuration mode

Usage Guide

Use this command to configure the URL of the CPE to which the ACS will connect. If no CPE URL is manually specified but a dynamic CPE URL is obtained through DHCP, the ACS initiates a connection to the CPE using the dynamically obtained CPE URL. The URL of the CPE should meet the following format requirements:

- The URL of the CPE is formatted as http://ip [: port]/ path.
- The URL of the CPE consists of at most 256 characters.

Configuration Examples

The following example specifies the URL of the CPE to http://10.10.10.1:7547/acs.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#cpe url Hhttp://10.10.10.1:7547/
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description

N/A

8.8 cpe username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS.

Use the **no** form of this command to restore the default setting.

cpe username *username*

no cpe username

Parameter Description

Parameter	Description
username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Defaults

N/A

Command Mode

CWMP configuration mode

Usage Guide

Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Configuration Examples

The following example configures the CPE username to be authenticated for the ACS to connect to the CPE to admin.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#cpe username admin
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
cpe password	Configures the CPE password to be authenticated for the ACS to connect to the CPE.

Platform Description

N/A

8.9 cwmp

Use this command to enable the CWMP function.

Use the **no** form of this command to disable this function.

cwmp

no cwmp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, this function is enabled.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable or disable the CWMP function.

Configuration Examples

The following example disables the CWMP function.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#no cwmp
FS(config)#
```

Related Commands

Command	Description

show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

8.10 disable download

Use this command to disable the function of downloading main program and configuration files from the ACS.

Use the **no** form of this command to restore the default setting.

disable download

no disable download

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the CPE can download main program and configuration files from the ACS.

Command Mode CWMP configuration mode

Usage Guide N/A

Configuration Examples The following example disables the function of downloading main program and configuration files from the ACS.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#disable download
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description N/A

8.11 disable upload

Use this command to disable the function of uploading configuration and log files to the ACS.

Use the **no** form of this command to restore the default setting.

disable upload

no disable upload

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the CPE can upload its configuration and log files to the ACS.

Command Mode

CWMP configuration mode

Usage Guide

Disables the function of uploading configuration and log files to the ACS.

Configuration Examples

The following example disables the function of uploading configuration and log file to the ACS.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#disable upload
FS(config-cwmp)#
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description

N/A

8.12 show cwmp configuration

Use this command to display the current configuration of CWMP.

show cwmp configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privilege EXEC mode

Usage Guide

Configuration

The following example displays the current configuration of CWMP.

Examples

```
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
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

Field	Description
CWMP Status	Running status of CWMP.
ACS URL	URL of the ACS。
ACS username	ACS username to be authenticated for the CPE to connect to the ACS.
ACS password	ACS password to be authenticated for the CPE to connect to the ACS.
CPE URL	URL of the CPE。
CPE username	CPE username to be authenticated for the ACS to connect to the CPE.
CPE pass ord	CPE password to be authenticated for the ACS to connect to the CPE.
CPE inform status	Status of CPE periodical notification function.
CPE inform interval	CPE periodical notification interval.
CPE wait timeout	Timeout period of CPE sessions.
CPE inform start time	The start time of periodical notification.
CPE download status	Indicates whether to download main program and configuration files from the ACS.
CPE upload status	Indicates whether to upload configuration files and log files to the ACS.
CPE back up status	Indicates whether backup and restoration of the main program and configuration file is enabled.
CPE back up delay time	Delay time of the backup and restoration of the main program and configuration files.

Related

Command	Description

Commands

show cwmp status	Displays the running status of CWMP.

Platform Description N/A

8.13 show cwmp status

Uses this command to display the running status of CWMP

show cwmp status

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the running status of CWMP.

```
FS#show cwmp status
CWMP Status                        : enable
Session status                     : Close
Last success session               : Unknown
Last success session time          : Thu Jan  1 00:00:00 1970
Last fail session                  : Unknown
Last fail session time             : Thu Jan  1 00:00:00 1970
Session retry times                : 0
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

Field	Description
CWMP Status	The running status of CWMP
Session status	The current status of the session between the CPE and the ACS
Last success session	The last success session type
Last success session time	The last success session time
Last fail session	The last failed session type
Last fail session time	The last failed session time
Session retry times	The number of session retransmission attempts

Related Commands

Command	Description

show cwmp configuration	Displays the current configuration of CWMP.

Platform Description

N/A

8.14 timer cpe-timeout

Uses this command to configure the session timeout period of the CPE.

timer cpe- timeout *seconds*

no timer cpe-timeout

Parameter Description

Parameter	**Description**
seconds	Sets the session timeout, in the range from 10 to 600 in the unit of seconds.

Defaults

By default, the session timeout period is 30 seconds.

Command Mode

CWMP configuration mode

Usage Guide

Use this command to configure the session timeout period of the CPE.

The maximum waiting period that the CPE has when the CPE failed to receive the ACS reply.

Configuration Examples

The following example configures the session timeout period of the CPE to 50 seconds.

```
FS#config terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#cwmp
FS(config-cwmp)#timer cpe-timeout 50
FS(config-cwmp)#
```

Related Commands

Command	**Description**
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform Description

N/A

9 Syslog Commands

9.1 clear logging

Use this command to clear the logs from the buffer in privileged EXEC mode.

clear logging

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.

Configuration Examples The following example clears the log packets from the memory buffer.

```
FS# clear logging
```

Related Commands

Command	Function
logging on	Turns on the log switch.
show logging	Displays the logs in the buffer.
logging buffered	Records the logs in the memory buffer.

Platform Description N/A

9.2 logging

Use this command to send the log message to the specified syslog server.

logging { *ip-address* } [**udp-port** *port*]

Use this command to delete the specified syslog server.

no logging { *ip-address* }

Use this command to restore the default port 514.

no logging { *ip-address* } **udp-port**

Parameter Description

Parameter	Description
ip-address	Sets the IP address of the host receiving log messages.
udp-port *port*	Sets the port number of the host receiving log messages. The default is 514.

Defaults No log message is sent to syslog server by default.

Command Mode Global configuration mode

Usage Guide This command is used to configure a syslog server to receive log messages from the device. You can configure up to five syslog servers, log messages are sent to all configured syslog servers simultaneously,

Configuration Examples The following example configures a syslog server with IP address 202.101.11.1.

```
FS(config)# logging 202.101.11.1
```

The following example configures a syslog server with IP address 10.1.1.100 and port number 8099.

```
FS(config)# logging 202.101.11.1 udp-port 8099
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.3 logging buffered

Use this command to set the memory buffer parameters (log severity, buffer size) for logs at global configuration layer. Use the **no** form of the command to disable recording logs in the memory buffer. Use the **default** form of this command to restore the default setting.

logging buffered [*buffer-size* | *level*]

no logging buffered

default logging buffered

Parameter Description

Parameter	Description
buffer-size	Size of the buffer is related to the specific device type: 1. For the kernel / aggregation switches, 4 K to 10 M bytes. 2. For the access switches, 4 K to 1 M Bytes. 3. For other devices, 4 K to 128 K Bytes.
level	Severity of logs, from 0 to 7. The name of the severity or the numeral can be used.

Defaults The buffer size is related to the specific device type.

1. kernel switches: 1 M Bytes;
2. aggregation switches: 256 K Bytes;
3. access switches: 128 K Bytes;
4. other devices: 4 K Bytes

The log severity is 7.

Command Mode

Global configuration mode

Usage Guide

The memory buffer for log is used in recycled manner. That is, when the memory buffer with the specified size is full, the oldest information will be overwritten. To show the log information in the memory buffer, run the **show logging** command in privileged user mode.

The logs in the memory buffer are temporary, and will be cleared in case of device restart or the execution of the **clear logging** command in privileged user mode. To trace a problem, it is required to record logs in flash or send them to Syslog Server.

The log information is classified into the following 8 levels (Table 1):

Table-1

Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy
Critical	2	Critical conditions
Errors	3	Error message
warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
informational	6	Descriptive information
Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level.

When the level of log information to be displayed on devices is specified, the log information at or below the set level will be allowed to be displayed.

⚠ After running the system for a long time, modifying the log buffer size especially in condition of large buffer may fails due to the insufficent availble continuous memory. The failure message will be shown. It is recommended to modify the log buffer size as soon as the system starts.

Configuration Examples

The following example allows logs at and below severity 6 to be recorded in the memory buffer sized 10,000 bytes.

```
FS(config)# logging buffered 10000 6
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Displays the logs in the buffer.
clear logging	Clears the logs in the log buffer.

Platform Description

N/A

9.4 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console in global configuration mode. Use the **no** form of this command to prohibit printing log messages on the console.

logging console [*level*]

no logging console

Parameter Description

Parameter	Description
level	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 1.

Defaults

The default is debugging (7).

Command Mode

Global configuration mode

Usage Guide

When a log severity is set, the log messages at or below that severity will be displayed on the console.

The **show logging** command displays the related setting parameters and statistics of the log.

Configuration Examples

The following example sets the severity of log that is allowed to be displayed on the console as 6:

```
FS(config)# logging console informational
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Displays the logs and related log configuration parameters in the buffer.

Platform Description

N/A

9.5 logging count

Use this command to enable the log statistics function in global configuration mode. Use the **no** form of this command to restore the default setting.

logging count

no logging count

Parameter Description

Parameter	Description
N/A	N/A

Defaults The log statistics function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command enables the log statistics function. The statistics begins when the function is enabled. If you run the **no logging count** command, the statistics function is disabled and the statistics data is deleted.

Configuration Examples The following example enables the log statistics function:

```
FS(config)# logging count
```

Related Commands

Command	Description
show logging count	Displays log information about modules of the system.
show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

9.6 logging facility

Use this command to configure the device value of the log information in global configuration mode. Use the **no** form of the command to restore the default setting.

logging facility *facility-type*

no logging facility

Parameter Description

Parameter	Description
facility-type	Syslog device value. For specific settings, refer to the usage guide.

Defaults The default is 23 if the RFC5424 format is enabled (Local7, local use).

The default is 16 if the RFC5424 format is disabled (Local0, local use).

Command Mode Global configuration mode

Usage Guide The following table (Table-2) is the possible device values of Syslog:

Numerical Code	Facility
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 syslogd
6 (lpr)	Line printer subsystem
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
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
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

The default device value of FSOS is 23 (local 7).

Configuration Examples

The following example sets the device value of **Syslog** as **kernel**:

```
FS(config)# logging facility kern
```

Related Commands

Command	Description
logging console	Sets the severity of logs that are allowed to be displayed on the console.

Platform Description

N/A

9.7 logging file

Use this command to save log messages in the log file, which can be saved in hardware disk, expanded FLASH, USB. Use the **no** form of this command to restore the default setting,

logging file { **flash:***filename* | **usb0:***filename* | **usb1:***filename* } [*max-file-size*] [*level*]

no logging file

Parameter

Parameter	Description

Description

flash	Saves the log file in expanded FLASH.
usb0	Saves the log file in USB0. This parameter is supported by the device with one USB connector and the USB extension device.
usb1	Saves the log file in USB1, This parameter is supported by the device with two USB connectors and the USB extension device.
filename	Sets the file name. The file type is omitted, which is fixed as txt.
max-file-size	Sets the maximum file size, in the range from 128K to 6M bytes, The default is 128K,
level	Sets the level of the log message saved in the log file, which can be either the level name or the level number. The default is 6. See Usage Guide for details.

Defaults Log messages are not saved in expanded FLASH by default.

Command Mode Global configuration mode

Usage Guide You can save log messages in expanded FLASH if you don’t want to transmit log messages on the network or there is no syslog server,

The log file cannot be configured with the suffix, which is fixed as txt.

If there is no expanded FLASH, the **logging file flash** command is hidden automatically and cannot be configured.

Keyword	Level	Description
Emergencies	0	Emergency case. The system fails to run.
Alerts	1	Problem that call for immediate solution.
Critical	2	Critical message.
Errors	3	Error message.
warnings	4	Alarm message.
Notifications	5	message that is normal but calls for attention.
informational	6	Descriptive message.
Debugging	7	Debugging message

Configuration Examples The following example saves the log message in expanded FLASH and sets file name, file size and log level to syslog.txt, 128K and 6 respectively.

```
FS(config)# logging file flash:syslog
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

9.8 logging file numbers

Use this command to set the number of log files written into FLASH. Use the **no** form of this command to restore the default setting.

logging file numbers *numbers*

no logging file numbers

Parameter Description

Parameter	Description
numbers	Sets the number of log files written into FLASH, in the range from 2 to 32.

Defaults The default is 16.

Command Mode Global configuration mode

Usage Guide The system does not delete previously generated log files even if you change this configuration, Therefore, you need to delete the log files manually to save FLASH size (you can send log files to the server through TFTP before that). For example, 16 log files are generated by default before you want to change the number to 2. New logs are overwritten constantly in log files indexed 0 to 1. However, log files indexed from 2 to 16 remain. You can delete these log files manually as needed.

Configuration Examples The following example sets the number of log files written into FLASH to 8.

```
FS(config)# logging file numbers 8
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.9 logging filter direction

Use this command to filter the log messages destined to a certain direction. Use the **no** form of this command to restore the default setting.

logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

no logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }

Parameter

Parameter	Description

Description

all	Log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server.
buffer	Log messages destined to the log buffer are filtered, including log messages displayed by running the **show logging** command.
file	Log messages destined to the log file are filtered.
server	Log messages destined to the log server are filtered.
terminal	Log messages destined to the console and the VTY terminal (including Telnet and SSH).

Defaults Log messages destined to all directions are filtered by default.

Command Mode Global configuration mode

Usage Guide In general, log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server. If you want to filter log messages destined to a certain direction, the terminal for instance, configure the **terminal** parameter.

Configuration Examples The following example filters log messages destined to the terminal (including the console and the VTY terminal).

```
FS(config)# logging filter direction terminal
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.10 logging filter rule

Use this command to configure the filter rule of the log message,

logging filter rule { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* | **single-match** [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*] }

Use this command to delete the "exact-match" filter rule.

no logging filter rule exact-match [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*]

Use this command to delete the "single-match" filter rule.

no logging filter rule single-match [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*]

Parameter Description

Parameter	Description
exact-match	Exact-match filter rule. Fill in all the following three parameters.
single-match	Single-match filter rule. Fill in one of the following three parameters.
module *module-name*	Module name.

mnemonic *mnemonic-name*	Mnemonic name.
level *level*	Log level,

Defaults No filter rule is configured by default,

Command Mode Global configuration mode

Usage Guide If you want to filter a specific log message, use the "exact-match" filter rule and fill in all three parameters, namely, module name, mnemonic name and log level.

If you want to filter a specific kind of log messages, use the "single-match" filter rule and fill in one of three parameters, namely, module name, mnemonic name and log level.

When configured with the same module name, mnemonic name or log level, the "single-match" filter rule has a higher priority than the "exact-match" filter rule,

Configuration Examples The following example configures the "exact-match" filter rule with parameters of module name LOGIN, log level 5 and mnemonic name LOGOUT.

```
FS(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level 5
```

The following example configures the "single-match" filter rule with the parameter of module name SYS.

```
FS(config)# logging filter rule single-match module SYS
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.11 logging filter type

Use this command to configure the filter type of log messages. Use the **no** form of this command to restore the default setting.

logging filter type { **contains-only** | **filter-only** }

no logging filter type

Parameter Description

Parameter	Description
contains-only	The log message containing the key word of the filter rule is printed.
filter-only	The log message containing the key word of the filter rule is filtered.

Defaults The default filter type is filter-only.

Command Mode Global configuration mode

Usage Guide

1. When too many log messages are printed, the terminal screen keeps being refreshed. If you are not concerned with these log messages, use the "filter-only" filter type to filter the log messages,
2. If you are concerned with certain log messages, use the "contains-only" filter type to print log messages containing the key word of the filter rule, so as to monitor whether certain events happen.

ⓘ In real operation, the contains-only and the fitler-only filter types cannot be configured at the same time.

ⓘ If you configure the filter direction and the filter type without configuring the filter rule, the log messages are not filtered.

Configuration Examples

The following example sets the filter type to contains-only.

```
FS(config)# logging filter type contains-only
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.12 logging flash flush

Use this command to write log messages in the system buffer into the flash file immediately.

logging flash flush

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

In general, the log messages are cached in the log buffer. Only when the buffer is full or the timer expires are log messages written into the flash file. This command is used to write log messages in the system buffer into the flash file immediately.

ⓘ The **logging flash flush** command takes effect only once for each configuration. The log messages cached in the buffer are written into the flash file immediately after configuration.

Configuration Examples

The following example writes log messages in the system buffer into the flash file immediately.

```
FS(config)# logging flash flush
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.13 logging flash interval

Use this command to set the interval to write log messages into the flash file, Use the **no** form of this command to restore the default setting.

logging flash interval *seconds*

no logging flash interval

Parameter Description

Parameter	Description
interval *seconds*	The interval to write log messages into the flash file, in the range from 1 to 57840 in the unit of seconds.

Defaults The default is 3600.

Command Mode Global configuration mode

Usage Guide This command is used to set the interval to write log messages into the flash file. The timer starts after configuration, If you want to restore the interval to 3600 seconds, use the **no logging flash interval** command.

To avoid writing log messages into the flash file too frequently, it is not recommended to set a short interval.

Configuration Examples The following example sets the interval to write log messages into the flash file to 300 seconds.

```
FS(config)# logging flash interval 300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.14 logging life-time

Use this command to configure the preservation duration of logs in expanded FLASH. Use the **no** form of this command to restore the default setting.

logging life-time level *level days*

no logging life-time level *level*

Parameter Description

Parameter	**Description**
level	Sets the log level, which can be either the level name or the level number.
days	Sets the preservation duration of logs.

Defaults No preservation duration is set by default.

Command Mode Global configuration mode

Usage Guide Due to difference in expanded FLASH size and log level, logs with different levels can be configured with different preservation durations.

Once log preservation based on time is enabled, log preservation based on file size is disabled automatically. The log files are stored under the syslog/ directory of the expanded FLASH,

Configuration Examples The following example sets the preservation duration of logs whose level is 6 to 10 days.

```
FS(config)# logging life-time level 6 10
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

9.15 logging monitor

Use this command to set the severity of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.) in global configuration mode. Use the **no** form of this command to disable this function.

logging monitor [*level*]

no logging monitor

Parameter Description

Parameter	**Description**
level	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table-1.

Defaults The default is debugging (7).

Command Mode

Global configuration mode

Usage Guide

To print log information on the VTY window, run the **terminal monitor** command in privileged EXEC mode. The level of logs to be displayed is defined by **logging monitor**.
The log level defined with "Logging monitor" is for all VTY windows.

Configuration Examples

The following example sets the severity of log that is allowed to be printed on the VTY window as 6:

```
FS(config)# logging monitor informational
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Displays the log messages and related log configuration parameters in the buffer.

Platform Description

N/A

9.16 logging on

Use this command globally to allow logs to be displayed on different devices. Use the **no** form of this command to disable this fucntion.

logging on

no logging on

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Logs are allowed to be displayed on different devices.

Command Mode

Global configuration mode

Usage Guide

Log information can not only be shown in the Console window and VTY window, but also be recorded in different equipments such as the memory buffer, the expanded FLASH and the Syslog Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is greater than 1.

Configuration Examples

The following example disables the log switch on the device.

```
FS(config)# no logging on
```

Related

Command	Description

logging buffered	Records the logs to a memory buffer.
logging server	Sends logs to the Syslog server.
logging file flash:	Records logs on the expanded FLASH.
logging console	Allows the log level to be displayed on the console.
logging monitor	Allows the log level to be displayed on the VTY window (such as telnet window) .
logging trap	Sets the log level to be sent to the Syslog server.

Platform Description

N/A

9.17 logging rate-limit

Use this command to enable log rate limit function to limit the output logs in a second in the global configuration mode. Use the **no** form of this command to disable this function.

logging rate-limit { *number* | **all** *number* | **console** { *number* | **all** *number* } } [**except** *severity*]

no logging rate-limit

Parameter Description

Parameter	Description
number	The number of logs that can be processed in a second in the range from 1 to 10000.
all	Sets rate limit to all the logs with severity level 0 to 7.
console	Sets the amount of logs that can be shown in the console in a second.
except	By default, the severity level is error (3). The rate of the log whose severity level is less than or equal to error (3) is not controlled.
severity	Log severity level in the range from 0 to 7. The lower the level is, the higher the severity is.

Defaults

The log rate limit function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to control the syslog outpt to prevent the massive log output.

Configuration Examples

The following example sets the number of the logs (including debug) that can be processed in a second as 10. However, the logs with warning or higher severity level are not controlled:

```
FS(config)#logging rate-limit all 10 except warnings
```

Related Commands

Command	Description
show logging count	Displays log information about modules of the system.

show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description

N/A

9.18 logging server

Use this command to send the logs to the specified Syslog Sever in global configuration mode. Use the **no** form of this command to remove the setting. Use the **default** form of this command to restore the default setting.

logging server [**oob**] { *ip-address* } | **ipv6** *ipv6-address* } [**udp-port** *port*]

no logging server [**oob**] { *ip-address* | **ipv6** *ipv6-address* }

no logging server { *ip-address* | **ipv6** *ipv6-address* } **udp-port**

Parameter Description

Parameter	Description
oob	Specifies out-of-band communication for the logging server. (logs are sent through the MGMT port to the logging server.)
ip-address	IP address of the host that receives log information.
ip-address	IP address of the host that receives log information.
udp-port *port*	Specifies the port number for the specified host (The default port number is 514).

Defaults

No log is sent to any syslog server by default.

Command Mode

Global configuration mode

Usage Guide

This command specifies a Syslog server to receive the logs of the device. Users are allowed to configure up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time.

Configuration Examples

The following example specifies a syslog server of the address 202.101.11.1:

```
FS(config)# logging server 202.101.11.1
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Displays log messages and related log configuration parameters in the buffer.
logging trap	Sets the level of logs allowed to be sent to Syslog server.

Platform Description N/A

9.19 logging source interface

Use this command to configure the source interface of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

logging source [**interface**] *interface-type interface-number*

no logging source [**interface**]

Parameter Description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.

Defaults No source interface is configured by default.

Command Mode Global configuration mode

Usage Guide By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique addresses. If the source interface is not configured on the device, or no IP address is configured for the source interface, the source address of the log messages is the address of the sending interface.

Configuration Examples The following example specifies loopback 0 as the source address of the syslog messages:

```
FS(config)# logging source interface loopback 0
```

Related Commands

Command	Description
logging server	Sends logs to the Syslog server.

Platform Description N/A

9.20 logging source ip

Use this command to configure the source IP address of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

logging source {**ip** *ip-address* }

no logging source { **ip** }

Parameter Description

Parameter	Description
ip-address	Specifies the source IPV4 address sending the logs to IPV4 log server.

Defaults No source address is configured by default.

Command Mode Global configuration mode

Usage Guide By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique addresses. If this IP address is not configured on the device, the source address of the log messages is the address of the sending interface.

Configuration Examples The following example specifies 192.168.1.1 as the source address of the syslog messages:

```
FS(config)# logging source ip 192.168.1.1
```

Related Commands

Command	Description
logging server	Sends the logs to the Syslog server.

Platform Description N/A

9.21 logging synchronous

Use this command to enable synchronization function between user input and log output in line configuration mode to prevent interruption when the user is keying in characters. Use the **no** form of this command to restore the default setting.

logging synchronous

no logging synchronous

Parameter Description

Parameter	Description
N/A	N/A

Defaults The synchronization function between user input and log output is disabled by default.

Command Mode Line configuration mode

Usage Guide This command enables synchronization function between user input and log output, preventing the user from interrupting when keying in the characters.

Configuration Examples

```
FS(config)#line console 0
FS(config-line)#logging synchronous
```

Print UP-DOWN logs on the port when keying in the command, the input command will be output again:

```
FS# configure terminal
Oct    9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to down
Oct    9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to
DOWN
FS# configure terminal//----the input command by the user is output again rather than being
intererupted.
```

Related Commands

Command	Description
show running-config	Displays the configuration.

Platform Description

N/A

9.22 logging trap

Use this command to set the severity of logs that are allowed to be sent to the syslog server in global configuration mode. Use the **no** form of this command to prohibit sending log messages to the Syslog server.

logging trap [*level*]

no logging trap

Parameter Description

Parameter	Description
level	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 1.

Defaults

The default is informational(6)

Command Mode

Global configuration mode

Usage Guide

To send logs to the Syslog Server, run the **logging** command in global configuration mode to configure the **Syslog Server**. Then, run the **logging trap** command to specify the severity level of logs to be sent.

The **show logging** command displays the configured related parameters and statistics of the log.

Configuration Examples

The following example enables logs at severity 6 to be sent to the Syslog Server with the address of 202.101.11.22:

```
FS(config)# logging 202.101.11.22
FS(config)# logging trap informational
```

Related Commands

Command	Description
logging on	Turns on the log switch.
logging	Sends logs to the Syslog server.

show logging	Displays the log messages and related log configuration parameters in the buffer.

Platform Description N/A

9.23 logging userinfo

Use this command to enable the logging function to record user log/exit. Use the **no** form of this command to restore the default setting.

logging userinfo

no logging userinfo

Parameter Description

Parameter	Description
N/A	N/A

Defaults No log message is printed recording user log/exit by default.

Command Mode Global configuration mode

Usage Guide This command is used to print the log message to remind the administrator of user login. The log message is in the format as follows:

```
Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0 (192.168.23.68) OK.
```

Configuration Examples The following example enables the logging function to record user log/exit.

```
FS(config)# logging user-info
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.24 logging userinfo command-log

Use this command to enable the logging function to record user operation. Use the **no** form of this command to restore the default setting.

logging userinfo command-log

no logging userinfo command-log

Parameter Description

Parameter	Description

N/A	N/A

Defaults No log message is printed recording user operation by default.

Command Mode Global configuration mode

Usage Guide This command is used to print the log message to remind the administrator of configuration change. The log message is in the format as follows:

```
Mar 22 14:10:40 %CLI-5-EXEC_CMD: Configured from vty0 (192.168.23.68) command-log: logging server 192.168.23.68.
```

Configuration Examples The following example enables the logging function to record user operation.

```
FS(config)# logging user-info command-log
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.25 service private-syslog

Use this command to set the syslog format to the private syslog format. Use the **no** form of this command to restore the default setting.

service private-syslog

no service private-syslog

Parameter Description

Parameter	Description
N/A	N/A

Defaults The syslog is displayed in the default format.

Command Mode Global configuration mode

Usage Guide By default, the syslog is displayed in the format as follows:

*timestamp: %facility-severity-mnemonic: description

Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:

timestamp facility-severity-mnemonic: description

Here is an example:

```
May 31 23:31:28 SYS-5-CONFIG_I: Configured from console by console
```

The difference between the private syslog format and the default syslog format lies in the following marks:

The private syslog does not have "*" before the timestamp, ":" after the timestamp and "%" before the identifying string.

Configuration Examples

The following example sets the private syslog format.

```
FS(config)# service private-syslog
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.26 service sequence-numbers

Use this command to attach serial numbers into the logs in global configuration mode. Use the **no** form of this command to restore the default setting.

service sequence-numbers

no service sequence-numbers

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No serial number is contained in the logs by default.

Command Mode

Global configuration mode

Usage Guide

In addition to the timestamp, you can add serial numbers to the logs, numbering from 1. Then, it is clearly known whether the logs are lost or not and their sequence.

Configuration Examples

The following example adds serial numbers to the logs.

```
FS(config)# service sequence-numbers
```

Related Commands

Command	Description
logging on	Turns on the log switch.
service timestamps	Attaches timestamps to the logs.

Platform

N/A

Description

9.27 service standard-syslog

Use this command to set the syslog format to the standard syslog format defined in RFC3164. Use the **no** form of this command to restore the default setting.

service standard-syslog

no service standard-syslog

Parameter Description

Parameter	Description
N/A	N/A

Defaults The syslog is displayed in the default format.

Command Mode Global configuration mode

Usage Guide By default, the syslog is displayed in the format as follows:

*timestamp: %facility-severity-mnemonic: description

Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:

timestamp %facility-severity-mnemonic: description

Here is an example:

```
May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console
```

The difference between the standard syslog format and the default syslog format lies in the following marks:

The standard syslog does not have “*” before the timestamp and “:” after the timestamp.

Configuration Examples The following example sets the standard syslog format.

```
FS(config)# service standard-syslog
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9.28 service sysname

Use this command to attach system name to logs in global configuration mode. Use the **no** form of this command to restore the default setting.

service sysname

no service sysname

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults

No system name is attached to logs by default.

Command Mode

Global configuration mode

Usage Guide

This command allows you to decide whether to add system name in the log information.

Configuration Examples

The following example adds a system name in the log information:

```
Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console
FS #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS (config)#service sysname
FS (config)#end
FS #
Mar 22 15:35:57 S3250 %SYS-5-CONFIG: Configured from console by console
```

Related Commands

Command	**Function**
show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description

N/A

9.29 service timestamps

Use this command to attach timestamp into logs in global configuration mode. Use the **no** form of this command to remove the timestamp from the logs. Use the **default** form of this command to restore the default setting.

service timestamps [*message-type* [**uptime | datetime** [**msec** | **year**]]]

no service timestamps [*message-type*]

default service timestamps [*message-type*]

Parameter Description

Parameter	**Description**
message-type	The log type, including **Log** and **Debug**. The **log** type indicates the log information with severity levels of 0 to 6. The **debug** type indicates that with severity level 7.
uptime	Device start time in the format of *Day*Hour*Minute*Second, for example, 07:00:10:41.

datetime	Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07.
msec	Current time of the device in the format of Month*Date*Hour*Minute*Second*milisecond, for example, Jul 27 16:53:07.299
year	Current time of the device in the format of Year*Month*Date*Hour*Minute*Second, for example, 2007 Jul 27 16:53:07

Defaults

The time stamp in the log information is the current time of the device. If the device has no RTC, the time stamp is automatically set to the device start time.

Command Mode

Global configuration mode

Usage Guide

When the **uptime** option is used, the time format is the running period from the last start of the device to the present time, in seconds. When the **datetime** option is used, the time format is the date of the current device, in the format of YY-MM-DD, HH:MM:SS.

Configuration Examples

The following example enables the timestamp for **log** and **debug** information, in format of Datetime, supporting millisecond display.

```
FS(config)# service timestamps debug datetime msec
FS(config)# service timestamps log datetime msec
FS(config)# end
FS(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I: configured from console by console
```

Related Commands

Command	Description
logging on	Turns on the log switch.
service sequence-numbers	Enables serial numbers of logs.

Platform Description

N/A

9.30 show logging

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from before to now.

show logging

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following command displays the result of the **show logging** command with RFC5424 format disabled.

```
FS# show logging
Syslog logging: enabled
    Console logging: level debugging, 15495 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 15496 messages logged
    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, 15242 message lines logged,0 fail
        logging to    202.101.11.22
        logging to    192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015487: *Sep 19 02:46:13: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015488: *Sep 19 02:46:13: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed
state to up.
015489: *Sep 19 02:46:26: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down.
015490: *Sep 19 02:46:26: FS %LINEPROTON/A5N/AUPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to down.
015491: *Sep 19 02:46:28: FS %LINKN/A3N/AUPDOWN: Interface FastEthernet 0/24, changed state to up.
015492: *Sep 19 02:46:28: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed
state to up.
```

Log information description:

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.

Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging** command with RFC5424 format enabled.

```
FS# show logging
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
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z FS - 7 - - Please config the IP address for capwap.
<132>1 2013-07-24T12:20:02.80313Z FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<135>1 2013-07-24T12:20:02.80343Z FS - 7 - - Please config the IP address for capwap.
<132>1 2013-07-24T12:20:32.250265Z FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<134>1 2013-07-24T12:29:33.410123Z FS SYS 6 SHELL_LOGIN [USER@4881 name="" type="" from="console"]
user login success.
<134>1 2013-07-24T12:29:34.343763Z FS SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal

Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

Related Commands

Command	Function
logging on	Turns on the log switch.
clear logging	Clears the log messages in the buffer.

Platform Description

N/A

9.31 show logging config

Use this command to display log configuration and statistics.

show logging config

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the outcome of running the **show logging config** command with RFC5424 disabled.

```
FS# show logging config
Syslog logging: enabled
    Console logging: level debugging, 15495 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 15496 messages logged
    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, 15242 message lines logged,0 fail
        logging to    202.101.11.22
```

```
     logging to     192.168.200.112
```

Field	Description
Syslog logging	Whether the logging function is enabled or disabled.
Console logging	The level and statistics of the log message printed on the console.
Monitor logging	The level and statistics of the log message printed on the VTY window.
Buffer logging	The level and statistics of the log message recorded in the memory buffer.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of debugging message.
Timestamp log messages	Timestamp format of log message.
Sequence-number log messages	Whether the sequence number function is enabled or disabled.
Sysname log messages	Adds the system name to the log message.
Count log messages	Log-counting function
Trap logging	The level and statistics of the log message sent to the syslog server.

The following example displays the outcome of running the **show logging config** command with RFC5424 enabled.

```
FS# show logging
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
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to output console and remove terminal

Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending way and statistics

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.32 show logging count

Use this command to display the statistics about occurrence times, and the last occurrence time of each module log in the system in privileged mode.

show logging count

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

To use the log packet statistics function, run the **logging count** command in global configuration mode. The **show logging count** command can show the information of a specific log, occurrence times, and the last occurrence time.

You can use the **show logging** command to check whether the log statistics function is enabled.

Configuration Examples

The following example displays the result of the **show logging count** command:

```
FS# show logging count
Module Name     Message Name Sev Occur        Last Time
SYS             CONFIG_I        5    1           Jul 6 10:29:57
SYS TOTAL                            1
```

Related Commands

Command	Function
logging count	Enables the log statistics function.
show logging	Displays basic configuration of log modules and log information in the buffer.
clear logging	Clears the logs in the buffer.

Platform Description N/A

9.33 show logging reverse

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from now to before.

show logging reverse

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide

Configuration Examples The following command displays the result of the **show logging reverse** command with RFC5424 format disabled.

```
FS# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  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, 15242 message lines logged,0 fail
    logging to   202.101.11.22
    logging to   192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015492: *Sep 19 02:46:28: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to up.
015491: *Sep 19 02:46:28: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015490: *Sep 19 02:46:26: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to down.
015489: *Sep 19 02:46:26: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down.
```

```
015488: *Sep 19 02:46:13: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed
state to up.
015487: *Sep 19 02:46:13: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging reverse** command with RFC5424 format enabled.

```
FS# show logging reverse
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
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<134>1 2013-07-24T12:29:34.343763Z FS SYS 6 SHELL_CMD [USER@4881 name=""][CMD@4881 task="rl_con"
cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z FS SYS 6 SHELL_LOGIN [USER@4881 name="" type="" from="console"]
```

```
user login success.
<132>1 2013-07-24T12:20:32.250265Z FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<135>1 2013-07-24T12:20:02.80343Z FS - 7 - - Please config the IP address for capwap.
<132>1 2013-07-24T12:20:02.80313Z FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<135>1 2013-07-24T12:19:33.130290Z FS - 7 - - Please config the IP address for capwap.
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.34 terminal monitor

Use this command to show logs on the current VTY window. Use the **no** form of this command to restore the default setting.

terminal monitor

terminal no monitor

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Log information is not allowed to be displayed on the VTY window by default.

Command Mode

Privileged EXEC mode

Usage Guide

This command only sets the temporary attributes of the current VTY. As the temporary attribute, it is not stored permanently. At the end of the VTY terminal session, the system will use the default setting, and the temporary setting is invalid. This command can be also executed on the console, but it does not take effect.

Configuration Examples

The following example allows log information to be printed on the current VTY window:

```
FS# terminal monitor
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Command History

Version	Description
N/A	N/A

9.35 logging language

Use this command to configure the syslog language. Use the **no** form of this command to restore the default settings.

logging language { **Chinese** | **English** }

no logging language

Parameter Description

Parameter	Description
Chinese	The language is Chinese.
English	The language is English.

Defaults

The default language is Chinese.

Defaults

The default language is English.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the syslog language to English.

```
FS(config)# logging language English
```

Related Commands

Command	Function
N/A	N/A

Platform Description	N/A

10 LED Commands

10.1 led on

Use this command to turn on LEDs for AP location.

Use the **no** form of this command to restore the default setting.

led on [**slot** *slot-id*]

no led on [**slot** *slot-id*]

Parameter Description

Parameter	Description
slot-id	Slot ID corresponding to the RF card

Defaults

This function is disabled by default.

Command Mode

AP configuration mode

Usage Guide

For rack APs, specify the slot ID for every RF card. For non-rack APs, the *slot-id* parameter is invalid.

Configuration Examples

The following example turns on LEDs for AP location.

```
FS(config)#ap-config 00d0.f822.33bc
FS(config-ap)#led on
```

The following example turns off LEDs for AP location.

```
FS(config)#ap-config 00d0.f822.33bc
FS(config-ap)#no led on
```

Platform Description

N/A

10.2 quiet-mode session

Use this command to configure LED quiet mode.

Use the **no** form of this command to restore the default setting.

quiet-mode session *session-num*

no quiet-mode session *session-num*

Parameter Description

Parameter	Description
session-num	Session ID.

Defaults

This function is disabled by default.

Command Mode

AP configuration mode

Usage Guide

Use this command to turn off all LEDs on the AP.

Configuration Examples

The following example configures LED quiet mode from 23:00 that night to 7:00 next day.

```
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
```

The following example disables LED quiet mode.

```
FS(config)#ap-config 00d0.f822.33bc
FS(config-ap)#no quiet-mode session 1
```

Platform Description

N/A

11 Exception Alarm Commands

11.1 feedback frequency

Use this command to configure a mailing frequency.

feedback frequency *min*

Use the **no** form of this command to restore the default configuration.

no feedback frequency

Parameter Description

Parameter	Description
frequency *min*	Indicates a mailing frequency in minutes. The value range is from 5 to 10,080. The default value is 60.

Defaults 60

Command Mode Global configuration mode

Usage Guide To receive emails as soon as possible, set this parameter to a small value. A smaller value indicates more timely receiving of emails. If there is a great amount of exception information, emails will be received frequently.

To avoid frequently receiving emails, set this parameter to a large value, for example, 1440 minutes. Then, exception information will be sent once a day. In this case, the administrator will not be notified in a timely manner if an exception occurs.

⚠ Set the mailing frequency as required.

Configuration Example #Set the mailing frequency to 120 minutes.

```
FS(config)# feedback frequency 120
```

Verification Run the **show run** command to display the configuration result.

11.2 feedback ignore item

Use this command to set the ID of an alarm option to be ignored.

feedback ignore-item *item-id*

Use the **no** form of this command to delete the configuration.

no feedback ignore-item *item-id*

Parameter Description

Parameter	Description
ignore-item *item-id*	Sets the ID of an alarm option to be ignored. The value range is from 0 to 8.

Defaults N/A

Command Mode Global configuration mode

Usage Guide

⚠ No exception about the ignored alarm option will be emailed to the administrator.

Configuration Example

#Set the mailing frequency to 120 minutes.

```
FS(config)# feedback frequency 120
```

Verification Run the **show run** command to display the configuration result.

11.3 feedback subscriber

Use this command to configure a receiving mailbox.

feedback subscriber *mail-addr*

Use the **no** form of this command to delete the configuration.

no feedback subscriber *mail-addr*

Parameter Description

Parameter	Description
subscriber *mail-addr*	Configures a receiving mailbox. A maximum of six receiving mailboxes can be configured.

Defaults N/A

Command Mode Global configuration mode

Usage Guide To send the exception information to multiple users by email, repeat the command.

Configuration Example

#Configure a recipient.

```
FS(config)# feedback subscriber FS@sina.com.cn
```

Verification Run the **show run** command to display the configuration result.

11.4 feedback user enable

Use this command to enable the exception alarm function.

feedback user enable

Use the **no** form of this command to disable the exception alarm function.

no feedback user enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Enable this function before using it.

The exception alarm function must be supported by the following functions at the same time:

- Mail service
- SMTP server
- Email sending address and password
- Receiving mailbox

Configuration Example

#Enable the exception alarm function.

```
FS(config)# feedback user enable
```

Verification

Run the **show run** command to display the configuration result.

11.5 mail-client check

Use this command to check email-related configurations.

mail-client check

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to check whether the SMTP server and email address and password are successfully configured. If yes, a test email will be received.

Configuration Example

#Check the email configuration.

```
FS# mail-client check
Connect to smtp server. OK!
Login to smtp server. OK!
```

```
Send a test mail. OK!
Check OK!
```

Verification Log in to the mailbox through a browser to check whether a test email is received.

11.6 mail-client smtp server

Use this command to configure an SMTP server.

mail-client smtp server *addr* [**port** *value*]

Use the **no** form of this command to delete the configuration.

no mail-client smtp server

Parameter Description

Parameter	Description
addr	Indicates the IP address of the SMTP server.
value	Indicates the port number of the SMTP server. The value range is from 1 to 65,535.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The SMTP server must be configured in order to send emails about exceptions.

The URL of the SMTP server can be queried from a mailbox website, for example, smtp.qq.com or smtp.126.com.

The SMTP service of some mailbox (for example, QQ email) is disabled by default. Log in to the mailbox through a browser, and enable the SMTP service.

Configuration Example #Configure an SMTP server.

```
FS(config)# mail-client server smtp.126.com
```

Verification Log in to the mailbox through a browser to check whether a test email is received.

11.7 mail-client username

Use this command to configure the email address and password.

mail-client username *mail-addr* **password** *pw-string*

Use the **no** form of this command to delete the configuration.

no mail-client username *mail-addr* **password** *pw-string*

Parameter Description

Parameter	Description

username *mail-addr*	Indicates an email address in the format of xxx@yyy. This command does not check the format.
password *pw-string*	Indicates a password.

Defaults N/A

Command Mode Global configuration mode

Usage Guide Check the following:

1. The email address is applied for from a commonly used mailbox website. At present, mailboxes that pass verification are suffixed by 163.com, 126.com, 139.com, sina.com, qq.com, and tom.com. Other unverified mailboxes may also be used.
2. The mailbox supports the SMTP service. The mailboxes mentioned above all support the SMTP service.
3. Log in to the mailbox through a browser to check whether the SMTP service is enabled.
4. Log in to the mailbox website to check the IP address of the SMTP server.

Configuration Example #Configure the email address and password.

```
FS(config)# mail-client username FS@qq.com password ******
```

Verification Run the **show run** command to display the configuration result.

11.8 mail-service enable

Use this command to enable the mail service.

mail-service enable

Use the **no** form of this command to disable the mail service.

no mail-service enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The mail service is enabled by default.

Command Mode Global configuration mode

Usage Guide Mail-related functions must be supported by the mail service.

Configuration Example #Enable the mail service.

```
FS(config)# mail-service enable
```

Verification Run the **show run** command to display the configuration result.

11.9 mail-service source

Use this command to configure a source IP address of the mail service.

mail-service source *ip*

Use the **no** form of this command to delete the source IP address of the mail service.

no mail-service source

Parameter Description

Parameter	**Description**
ip	Indicates the source IP address.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The source IP address must be configured in public network mode, and it is generally set to the IP address of an intranet port.

Configuration Example #Set the source IP address of the mail service to 1.1.1.1.

```
FS(config)# mail-service source 1.1.1.1
```

Verification Run the **show run** command to display the configuration result.

11.10 show feedback items

Use this command to display the alarm options.

show feedback items

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide Use this command to display the alarm options supported by the gateway.

Configuration Example #Display the alarm options supported by the gateway.

```
FS#show feedback items
no.   name                                   ignore
------------------------------------------
4,    high CPU temperature,                         NO
```

```
5,     device attack,                        NO
6,     total bandwidth exceeding the limit,                  NO
7,     flow control exception,                        NO
8,     high main board temperature,                      NO
```

Field description:

Field	Description
no.	Indicates an option ID.
name	Indicates an option name.
ignore	Ignores the option.

12 HTTP Service Commands

12.1 enable service web-server

Use this command to enable the HTTP service function.

Use the **no** or **default** form of this command to disable the HTTP service function.

enable service web-server [**http** | **https** | **all**]

no enable service web-server [**http** | **https**]

default enable service web-server [**http** | **https**]

Parameter Description

Parameter	Description
http	Enables the HTTP service.
https	Enables the HTTPS service.
all	Enables both the HTTP service and the HTTPS service.

Defaults By default, the HTTP service function is disabled.

Command mode Global configuration mode.

Usage Guide If run a command ends with the keyword **all** or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword **http**, it indicates enabling the HTTP service; if run a command ends with keyword **https**, it indicates enabling the HTTPS service. Use the command **no enable service web-server** to disable the corresponding HTTP service.

Configuration Examples The following example enables both the HTTP service and the HTTPS service:

```
FS(config)#enable service web-server
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.2 http check-version

Use this command to detect the available upgrade files on the HTTP server.

http check-version

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

Use this command to detect the available upgrade files. The detected upgrade files version is later than that of local files.

Configuration Examples

The following example demonstrates the version of the detected HTTP upgrade file.

```
FS# http check-version
Business modules need to be updated: character-db, route-db
app name:web
    app-name              version               filename
--------------- -------------------- ------------------------
character-db       2014.02.09.14.02.09 app_sub_1.exe
character-db       2014.02.09.14.02.09 app_file_list.txt
character-db       2014.02.09.14.02.09 app_sub_3.exe
character-db       2014.02.09.14.02.09 app_sub_2.exe
route-db            2013.12.01.00          route-choose.db
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.3 http update

Use this command to manually upgrade files.

http update { **all** | *string* }

Parameter Description

Parameter	Description
string	Name of the service to be upgraded. You can enter multiple services, and separate them with spaces.
all	Upgrade all services.

Defaults

N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example upgrades the route-db and url-db files.

```
FS# http update route-db
Downloading updated files, please wait...
Press Ctrl+C to quit
route-db: download and notify successfully.
```

Related Commands

Command	Description
http check-vesion	Detects the available update package on the HTTP server.

Platform Description N/A

12.4 http update mode

Use this command to configure the HTTP upgrade mode to manual mode. Use the **no** form of this command to restore the default upgrade mode, namely, auto mode.

http update mode manual

no http update mode

Parameter Description

Parameter	Description
manual	Configures the manual upgrade mode.

Defaults The default update mode is auto mode.

Command mode Global configuration mode.

Usage Guide Use this command to configure the HTTP upgrade mode to manual mode.

Configuration Examples The following example enables manual HTTP upgrade mode:

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#http update mode manual
```

Related

Command	Description

Commands

N/A	N/A

Platform Description

N/A

12.5 http update server

Use this command to configure the IP address and the HTTP port number of the HTTP server.

http update server { *host-name* | *ip-address* } [**port** *port-number*]

no http update server

Parameter Description

Parameter	Description
host-name	Host name of the HTTP server.
ip-address	IP address of the HTTP server.
port-number	Port number of the HTTP server. The range is from 1 to 65,535.

Defaults

By default, the IP address of the HTTP remote upgrade server is 0.0.0.0 and the port number is 80.

Command mode

Global configuration mode.

Usage Guide

Use this command to configure the IP address and the HTTP port number of the HTTP server. When processing upgrade, the user-configured server address is preferentially used. If the connection fails, the server address in store in the local upgrade record file will be used to establish the connection. When all the above connection fails, upgrade will be suspended.

At least one IP address of upgrade server is stored in the local upgrade record file, and this IP address cannot be modified.

⚠ The HTTP upgrade server address is not need to be configured because the local upgrade record file records available upgrade server addresses.

If the server domain needs to be configured, enable the DNS function on the device and configure the DNS server address.

Configuration Examples

The following example configures the IP address and the HTTP port number of the HTTP server:

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#http update server 10.83.132.1 port 90
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

12.6 http update set oob

Use this command to enable HTTP upgrade on the MGMT port. Use the **no** form of this command to restore the default setting.

http update set oob

no http update set oob

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, HTTP upgrade is performed on the common port.

Command mode Global configuration mode.

Usage Guide This command is supported only on the device supporting the MGMT ports.

Configuration Examples The following example enables HTTP upgrade on the MGMT port:

```
FS(config)# http update set oob
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.7 http update time

Use this command to configure the HTTP auto-detection time. Use the **no** form of this command to restore the default auto-detection time.

http update time daily *hh:mm*

no http update time

Parameter Description

Parameter	Description
hh:mm	Specified auto-detection time; (24-hour system); accurate to minute.

Defaults

The default HTTP auto-detection time is random.

Command mode

Global configuration mode.

Usage Guide

Use this command to configure the HTTP auto-detection time. The device detects the files available for upgrade on the server at the specified detection time. Use can read these detected file information through Web interface. Use the **no** form of this command to reset the auto-detection time as random.

Configuration Examples

The following example configures the HTTP auto-detection time：

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#http update time daily 23:40
```

Related Commands

Command	Description
http update mode	Configures the HTTP update mode

Platform Description

N/A

12.8 ip http port

Use this command to configure the HTTP port number.

Use the **no** form of this command to restore the default HTTP port number.

ip http port *port-number*

no ip http port

Parameter Description

Parameter	Description
port-number	Configures the HTTP port number. The value includes 80, 1025 to 65,535.

Defaults

The default HTTP port number is 80.

Command mode

Global configuration mode.

Usage Guide

Use this command to configure the HTTP port number.

Configuration Examples

The following example configures the HTTP port number as 8080:

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#ip http port 8080
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.9 ip http secure-port

Use this command to configure the HTTPS port number.

Use the **no** form of this command to restore the default HTTPS port number.

ip http secure-port *port-number*

no ip http secure-port

Parameter Description

Parameter	Description
port-number	Configures the HTTPS port number. The value includes 443, 1025 to 65,535.

Defaults

The default HTTP port number is 443.

Command mode

Global configuration mode.

Usage Guide

Use this command to configure the HTTPS port number.

Configuration Examples

The following example configures the HTTPS port number as 4443:

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#ip http secure-port 4443
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.
show web-server status	Displays the configuration and status of the Web service.

Platform Description

N/A

12.10 show web-server

Use this command to display the configuration and status of the Web service.

show web-server

Parameter

Parameter	Description

Description

N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the configuration and status of the Web service:

```
FS# show web-service
webservice:
    http          : enable
                   : port(80)
    https         : enable
                   : port(4430)
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.
http port	Configures the HTTP port number.
http secure-port	Configures the HTTPS port number.

Platform Description

N/A

13 PATCH-UPGRADE Commands

13.1 patch-upgrade

Use this command to set the patch upgrade mode to automatic or manual.

patch-upgrade set-mode { **auto** | **manual**}

Use this command to set the automatic patch loading period.

patch-upgrade set-active-time start *hh:mm* **end** *hh:mm*

Use this command to set manual patch upgrade.

patch-upgrade manual-active

Use this command to set manual patch uninstallation and deletion.

patch-upgrade delete

Parameter Description

Parameter	Description
hh:mm	Specifies the hour and minute.

Defaults The automatic patch upgrade mode is enabled by default, and the default automatic patch loading period is 03:00 to 04:00 every day.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide If the automatic patch upgrade mode is used, the patch package is automatically installed and loaded.

Manual patch upgrade can be performed only when the device has downloaded and installed a patch package.

Configuration Examples The following example sets automatic patch upgrade.

```
FS# patch-upgrade set-mode auto
```

The following example sets the automatic patch loading period to 12:00–13:00.

```
FS# patch-upgrade set-active-time start 12:00 end 13:00
```

Verification Run the **show patch-upgrade state** command to display the configuration.

13.2 show patch-upgrade state

Use this command to display configuration and status of PATCH-UPGRADE.

show patch-upgrade state

Parameter Description

Parameter	Description

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to display the status and configuration of PATCH-UPGRADE.

Configuration Examples

The following example displays the status and configuration of PATCH-UPGRADE.

```
FS# showpatch-upgrade state
show patch update info:
----------------------------
mode                    :auto
patch state         :uninstall
next state          :
outer state         :
active time         :NULL
check start         :03:00
check end             :04:00
check quiet          :5
need reboot          :0
version                :notpatch
per version         :notpatch
----------------------------
```

13.3 show patch-upgrade log

Use this command to display logs of PATCH-UPGRADE.

show patch-upgrade log

Parameter Description

Parameter	Description

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to display logs of PATCH-UPGRADE.

Configuration Examples

The following example displays logs of PATCH-UPGRADE.

```
FS# show patch-upgrade log
show patch log info
2017-08-16 11:49:32, [auto] patch install success
2017-08-16 12:00:03, [auto] patch active success
2017-08-16 14:04:43, [manual] patch running success
2017-08-16 17:12:33, [manual] patch install fail
2017-08-16 17:16:53, [manual] patch install success
2017-08-16 17:16:53, [manual] patch active success
2017-08-16 17:16:54, [manual] patch running success
2017-08-16 17:21:43, [manual] patch install fail
2017-08-16 17:31:37, [manual] patch install fail
2017-08-16 17:35:56, [manual] patch install fail
```

…

14 WEB-UPGRADE Commands

14.1 web-upgrade

Use this command to install and upgrade the web package in the local file system.

web-upgrade *url* [force]

Parameter Description

Parameter	Description
url	Indicates the local path for storing the web package.
force	Indicates that an upgrade is forcibly performed without considering version comparison.

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to upgrade the web package locally.

Before running this command, copy the web package to a specific directory of the device's file system.

When running this command, locate the web package based on the input path and upgrade it.

The following table lists available URL formats.

Parameter	Description
tmp:*url*	Path **/tmp/vsd/0/**
path *url*	Custom local file path

By default, an upgrade is not performed when the web package versions are the same. To ignore version comparison, carry the **force** parameter.

Configuration Examples The following example upgrades 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.
```

Verification Run the **show web-upgrade** command to display web package information. If the information is updated, the upgrade is successful.

Common Errors The web package path or name is incorrect.

14.2 show web-upgrade

Use this command to display version information of the web package.

show web-upgrade

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, or interface configuration mode

Default Level

N/A

Usage Guide

N/A

Configuration Examples

The following example displays version information of the web package.

```
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
```

The package information fields are described below.

Field	Description
Version	Package version
Md5	MD5 of the package
Size	Package size
Build	Package compilation and generation time
Compatible	Product models supported by the package
Incompatible	Product models not supported by the package

Chapter 3 Behavior Management Commands

1 Layer2/3 Classification Commands

1.1 clear subs-mab

Use this command to clear the bound MAC addresses in the subs perception-free mode.

clear subs-mab { **all** | **mac** *mac-addr* }

Parameter Description

Parameter	Description
mac-addr	Specifies MAC addresses bound after WEB authentication is successful.

Command Mode Privileged EXEC mode

Default level 14

Usage Guide After WEB authentication is successful, MAC addresses of terminals are bound. Run this command to clear those MAC addresses. As a result, authentication in the subs perception-free mode fails and a new round of WEB authentication is triggered.

Configuration Examples

1. #Use this command to clear all bound MAC addresses.

```
FS#clear subs-mal all
```

2. #Use this command to clear a specific bound MAC address.

```
FS#clear subs-mal mac 00d0.f822.cc33
```

Verification N/A

Common Errors Layer23 is not enabled, and policies of traffic control and audit based on STA are disabled.

1.2 layer23 classify enable

Use this command to enable layer 2 and layer 3 global recognition by classification.

layer23 classify enable

Use the **no** form of this command to disable the function.

no layer23 classify enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Layer23 classification is enabled by default.

Command Mode Global configuration mode

Default level 14

Usage Guide Layer23 classification supports object recognition based on VID, source IP or source MAC, or destination IP.

Configuration Examples

1. #Use this command to enable layer23 classification.

```
FS(config)# layer23 classify enable
```

2. #Use the **no** form of this command to disable the function.

```
FS(config)# no layer23 clas
```

Verification

1: Use the **show run | in layer23** command displaying **layer23 classify enable** to display whether the current configuration enables layer23 classification.

2: Use the **show layer23 obj-info** command to display whether layer23 classification is enabled in the kernel.

Common Errors Layer23 is not enabled, and policies of traffic control and audit based on STA are disabled.

1.3 layer23 deny-mode enable

Use this command to enable layer 2 and layer 3 global deny mode.

layer23 deny-mode

Use the **no** form of this command to disable the function.

no layer23 deny-mode enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Layer23 deny-mode is disabled by default.

Command Mode Global configuration mode

Default level 14

Usage Guide Layer23 deny-mode drops all packets by default, except the STA object added to the whitelist (i.e. eliminating denied STA).

Configuration Examples

1: #Use this command to enable layer23 deny-mode.

```
FS(config)# layer23 deny-mode enable
```

2: #Use **no** form of this command to disable the function.

```
FS(config)# no layer23 deny-mode enable
```

Verification

1: Use the **show layer23 deny-mode** command to display whether layer23 deny-mode is enabled or not.

2: Use the **show run | in layer23** command displaying **layer23 deny-mode enable** to display whether layer23 deny-mode is enabled in global configuration mode.

3: Use the **show layer23 obj-info** command to display whether layer23 deny-mode is enabled in the kernel.

1.4 layer23 flow-detect

Use this command to enable layer 2 and layer 3 flow detection and configure detection flow and time interval in global configuration mode.

layer23 flow-detect { enable | flow *flowrate* **| time-interval** *time* **}**

Use the **no** form of this command to disable off-line state detection by flow.

no layer23 flow-detect { enable | flow *flowrate* **| time-interval** *time* **}**

Parameter Description

Parameter	Description
flowrate	Sets flow rate
time	Sets time

Defaults

Layer23 off-line flow-detect is disabled by default.

Command Mode

Global configuration mode

Default level

14

Usage Guide

By enabling layer23 flow-detect, once the flow is under the configured flow threshold in a specific time interval, the IP endpoint and the account on-line via device authentication will be automatically kicked off the line by the device; and if the IP endpoint communicates with a third party, then the third party will receive the off-line packet.

Configuration Examples

1: #Enable layer23 flow-detect and set the time interval to 30 minutes for off line by zero flow.

```
FS(config)# layer23 flow-detect enable
FS(config)# layer23 flow-detect flow 0
FS(config)# layer23 flow-detect time-interval 30
```

2: #Use **no** form of this command to disable layer23 flow-detect.

```
FS(config)# no layer23 flow-detect
```

Verification

1: Use the **show layer23 flow-detect** command to display whether flow-detect is enabled and configurations of parameters.

2: Enable layer23 flow-detect after getting on-line by passing the authentication of the internal local portal, and set the time interval to 15minutes for off line by zero flow. If the IP of the STA is changed, the STA will be automatically kicked off the line by the device after 15 minutes without flow.

1.5 layer23 sam-accip-relate enable

Use this command to enable layer 2 and layer 3 SAM+ accounts association with group names in global configuration mode.

layer23 sam-accip-relate enable

Use the **no** form of this command to disable the function.

no layer23 sam-accip-relate enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Layer23 sam-accip-relate is disabled by default.

Command Mode Global configuration mode

Default level 14

Usage Guide By using the function, layer23 will identify the real-name information synchronized from SAM+ server, including IP, account and group. Because the device name is exclusive and belongs to only one parent group, it is recommended to make up account name in **Group:Name:Account** form at the device to assure the name is exclusive. This function is available only for users synchronized by SAM+ server.

Configuration Examples

1: #Use this command to enable Layer23 sam-accip-relate.

```
FS(config)# layer23 sam-accip-relate enable
```

2: #Use the **no** of this command to disable the function.

```
FS(config)# no layer23 sam-accip-relate enable
```

Verification

1: Use the **show layer23 sam-acc** command to display whether layer23 sam-accip-relate is enabled or not.

2: Use the **show run | in layer23** command displaying **layer23 sam-accip-relate** to display whether the current configuration enables the same account in SAM+ server to different groups.

3: After synchronizing the SAM+ account to the device, run the **show auth-subs brief** command to display whether the name is combined with the group name.

1.6 layer23 scc-attention enable

Use this command to enable SCC real-name information setting switch.

layer23 scc-attention enable

Use the no form of the command to disable this function.

no layer23 scc-attention enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, this function is enabled.

Command Mode Global configuration mode

Default level 14

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 1: #Enable SCC real-name information setting switch.

```
FS(config)# layer23 scc-attention enable
```

2. #Disable SCC real-name information setting swtich.

```
FS(config)# no layer23 scc-attention enable
```

Verification Use the **show layer23 state** command to display whether the function is enabled or not.

Use the **show run | in layer23** command to see whether **layer23 scc-attention enable** is displayed. If it is displayed, the function is enabled.

Prompt Information N/A

Common Errors N/A

1.7 layer23 strict-verification enable

Use this command to enable the strict verification mode and bind the IP address and MAC address of the test account.

layer23 strict-verification enable

Use the **no** form of the command to disable the verification mode.

no layer23 strict-verification enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, this feature is disabled.

Command Mode Global configuration mode

Default level 14

Usage Guide

In this mode, packets from a client with the static ARP entry unbound or incorrectly bound will be directly discarded.

Configuration Examples

1: #Enable the strict verification mode and bind the IP address and MAC address of the test account.

```
FS(config)# layer23 strict-verification enable
```

2: #Disable the strict verification mode.

```
FS(config)# no layer23 strict-verification enable
```

Verification

Run the **show layer23 strict-verification** command to check whether the strict verification mode switch is enabled.

Run the **show run | in strict** command to check whether the strict verification mode switch is enabled. If "layer23 strict-verification enable" is displayed, the mode is enabled.

Prompt Information

N/A

Common Errors

N/A

1.8 layer23 subs-mab enable

Use this command to enable the subs perception-free mode.

layer23 subs-mab enable

Use the **no** form of the command to restore the default setting.

no layer23 subs-mab enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, this feature is disabled.

Command Mode

Global configuration mode

Default level

14

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 Examples

1: #Enable the subs perception-free mode.

```
FS(config)# layer23 subs-mab enable
```

2: #Disable the subs perception-free mode.

```
FS(config)# no layer23 subs-mab enable
```

Verification

Run the **show subs-mab state** command to check whether the subs perception-free mode switch is enabled.

Run the **show run | in subs-mab** command to check whether the s subs perception-free switch is enabled. If "layer23 subs-mab enable" is displayed, the mode is enabled.

Prompt Information

N/A

Common Errors

N/A

1.9 network-group

Use this command to change the parent path of a child network.

network-group *str1* **move to parent** *str2*

Parameter Description

Parameter	Description
str1	Name of the child network to be moved
str2	Name of the parent network of the moved child network

Defaults

N/A

Command Mode

Privileged EXEC mode

Default level

14

Usage Guide

This command is used to change the path of a child network without changing other attributes of it and the layered structures of its child networks

Configuration Examples

1: #Move User A originally under the root directory to Group 1.

```
FS# network-group userA move to parent group1
```

Verification

Use the **show network-group brief** command to display whether the layered structure query of the current child network is successfully moved.

Prompt Information

1: Cannot find the name of the child network to be moved.

```
cannot find the child-network.
```

2: Cannot find the name of the parent network of the moved child network.

```
cannot find the parent-network.
```

3: Cannot move to parent of yourself.

```
cannot move to parent of yourself.
```

4: Cannot move the root

```
cannot move the root.
```

5: Needn't to move the child-network to its original parent-network.

```
the network needn't to be moved.
```

6: Child networks of the non-group parent cannot be moved.

```
childs of the range-network cannot be moved.
```

7: The parent of the moved child network should be the network group.

```
the parent after changed should be the network group!
```

8: Cannot move to the child network of yourself.

```
cannot move to the child of yourself.
```

9: The depth of the network structure is more than 5!

```
the depth of the network moving is more than 5!
```

10: Cannot move the system default group.

```
cannot move the system default group.
```

Common Errors

1: The depth of network structure after movement surpasses the limitation, which leads to the movement failure.

2: The system default group cannot be moved.

1.10 network-group export

Use this command to export configuration of networks in the current system into an external file.

network-group export { **txt** | **csv** } *filename*

Parameter Description

Parameter	Description
filename	File name

Defaults N/A

Command Mode Privileged EXEC mode

Default level 14

Usage Guide

This command is mainly to export in batches the configuration of networks in the current system into an external file.

Configuration Examples

1: #Export network configuration into file "ip-info.txt".

```
FS# network-group export txt ip-info.txt
```

Verification

Use the commands **show network-group all** and **show network-group brief**, and then open the **ip-info.txt** to display whether the current configuration is exported into the file.

1.11 network-group import

Use this command to import a network into the current configuration.

network-group import { **txt** | **csv** } *filename* [**overwrite**]

Parameter Description

Parameter	Description
filename	File name
overwrite	Flag of Collision mode

Defaults

N/A

Command Mode

Privileged EXEC mode

Default level

14

Usage Guide

This command is mainly to import network in batches into the current configuration.

The syntax to write network 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 with ","; for example, the last column does not exist, then leave "," in the end of this column.

The following is an example of a network record in a ".txt" format file:

/ 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 should be: one record with 4 columns, including parent-network path, child-network name and child-network IP address.

In normal mode, networks in collision will fail to create the file. In overwrite mode, all networks in collision will be eliminated, including collision in name and IP, and then a new network will be created.

Configuration Examples

1: #Import a network file "ip-info.txt".

```
FS# network-group import txt ip-info.txt
```

Verification

Use the commands **show network-group al**l and **show network-group brief** to display whether the current configuration contains the networks successfully imported.

1.12 network-group name

Use this command to configure networks.

network-group name *namestr* [**parent** *parent*] [**ip-host** *ip-addr* | **ip-subnet** *subnet mask* | **ip-range** *start end*]]

Use the **no** form of this command to eliminate networks.

no network-group name *namestr*

Parameter Description

Parameter	Description
namestr	Name of the network
parent	Path of the parent network
ip-addr	IP address of a single IP network
subnet	Start address of IP segment
mask	mask
start	Start address of IP range
end	End address of IP range

Defaults

System creates Out-Server networks by default.

Command Mode

Global configuration mode

Default level

14

Usage Guide

The network 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 layer23 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 the parent filed is not set, then the parent network will be under the root by default.

The name of a network is exclusive. Names of different networks cannot be the same.

Configuration Examples

1: #Configure IP address segment network "Network 1", containing IP segment 192.168.196.0, whose parent network is "User group 1" and the parent network of "User group 1" is "All users group".

```
FS(config)# network-group name network1 parent /all user-group/user-group1 ip-subnet 192.168.196.0
255.255.255.0
```

Verification

Use the **show network-group all** command to display all information about the network.

Prompt Information

1: Cannot find this network.

```
cannot find this network!
```

2: Cannot delete the default network group.

```
cannot delete the network default group.
```

3: Path of the parent network is wrong.

```
Parent string error.
```

4: Configuration of the parent subscriber is wrong.

```
parent subscriber error.
```

5: The name conflicts with xxx.

```
name conflict with xxx.
```

6: Cannot exchange network group and network.

```
network group and network cannot exchange
```

7: Conflicts with xxx in IP configuration.

```
ip conflict with xxx.
```

8: IP address errors.

```
ip address error.
```

9: The parent of IP range network must be a network group.

```
parent of ip range network must be network group.
```

10: IP address or mask errors.

```
ip or mask error
```

1.13 network-group rename

Use this command to rename the network.

network-group rename *oldname newname*

Parameter Description

Parameter	Description

oldname	Original name of the network
newname	New name of the network

Defaults N/A

Command Mode Privileged EXEC mode

Default level 14

Usage Guide This command is mainly to change the name of a network without changing other attributes of the original network.

Configuration Examples 1: #Rename the network group User A the User B.

```
FS# network-group rename userA userB
```

Verification Use the **show network-group by-name** *userB* command to display whether other attributes of the network group were changed after the network group is renamed.

Prompt Information 1: New name already exists.

```
name is conflict with other network.
```

2: Cannot find the original network.

```
cannot find this network
```

3: Cannot rename the system default network group.

```
cannot rename the network default group.
```

1.14 show auth-subs

Use this command to display the authenticated subscribers.

show auth-subs [**all** | **brief** | **parent** [*name* | **root**]]

Parameter Description

Parameter	Description
all	Displays the account information of all authenticated subscribers.
brief	Displays the layered structure of authenticated accounts
parent	Displays the child network information of authenticated accounts.
name | **root**	Name or root of the authenticated account

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide This command is used to display various configuration information of the authenticated subscribers via specified keywords.

Configuration Examples

1: #Displays the information of all authenticated accounts.

```
name                                                               dir type inde
smp_root                                                           1    2    2
sam_root                                                           1    4    3
webauth_root                                                       1    1    4
```

Field Interpretation

Field	Description
name	Name of authenticated subscribers
dir	Attribute of the authenticated subscriber group
type	Type of authenticated subscribers (1-auth, 2-smp, 3-smp+auth, 4-sam)
index	Index of authenticated subscribers, exclusive

N/A

1.15 show network-group

Use this command to display network group information.

chow network-group [**all** | **brief** | **parent** [*name* | **root**]]

Parameter Description

Parameter	Description
all	Displays all network information
brief	Displays layered structure of networks
parent	Displays child network information of the network
name | **root**	Name or root of the network

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide This command is used to display various configuration information of the network group via specified keywords.

Configuration Examples

1: #Display detailed information of all network groups.

```
name                                         dir index ip
root                                         1   1
Out_Server                                   1   2
li                                           1   18093
```

```
jj                                                      1    14691
uu                                                      0    32105 6.6.6.3 - 6.6.6.5
uuii                                                    1    12652
```

Field Interpretation

Field	Description
name	Name of the network
dir	Attribute of the network group
index	Index of the network, exclusive
IP	Configure IP address of the network

1.16 show subscriber

Use this command to display information of the subscriber.

show subscriber [**all** | **brief** | **parent** [*name* | **root**]

Parameter Description

Parameter	Description
all	Displays information of all subscribers
brief	Displays layered structure of the subscriber
parent	Displays the child network information of the subscriber
name | **root**	Name or root of the subscriber

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide This command is to display various configuration information of subscribers via specified keywords.

Configuration Examples

1: #Display detailed information of all subscribers.

```
name                                    mac              dir av-fc av-con vip rel deny pwd-e au-deny login
vpn vbr webauth ssl-deny bind h-pwd idx          ssl-radius ip
root                                  0000.0000.0000   1    0     0      0   0   0    0     0       0
1   0   1   0   0   0   1           0
Default_Group                         0000.0000.0000   1    0     0      0   0   0    0     0       0
1   0   1   0   0   0   2           0
without_auth_user                     0000.0000.0000   0    0     0      0   0   0    0     0       0
0   0   1   0   0   1   4           0
xxy                                   0000.0000.0000   1    0     0      0   0   0    0     0       0
1   0   1   0   0   0   549939033 0
tt                                    0000.0000.0000   0    0     0      1   0   0    0     0       0
1   0   1   0   2   0   3445540573 0           3.3.3.6
```

```
Vpn_Group                         0000.0000.0000   1    0     0      0   0   0    0     0
0      1   0   1   0    0    0      3         0
Department 5                            0000.0000.0000   1    0     0      0   0   0    0     0
0      1   0   1   0    0    0      912778062 0
ee                              0000.0000.0000   0    0     0      0   1   0    0     0     0
1   0   1   0    2    0      680907908 0          192.168.3.81
xhl                             0000.0000.0000   0    0     0      0   0   0    0     0     0
1   0   1   0    2    0      310883589 0          172.18.3.81
eg                              0000.0000.0000   0    0     0      0   0   0    0     0     0
1   0   1   0    2    0      2753766751 0          172.18.3.100 - 172.18.3.250
uiiu                            3333.3333.3333   0    0     0      0   0   0    0     0     0
1   0   1   0    1    1      2364943795 0
ttt                             0000.0000.0000   1    0     0      0   0   0    0     0     0
1   0   1   0    0    0      1938928104 0
```

Field Interpretation

Field	Description
name	User name
mac	Configured mac address
dir	Attribute of the user group
av-fc	Flag of traffic control free
av-con	Flag of identification and audit free
vip	VIP flag
rel	Flag of whitelist attributes
deny	Flag of deny attributes
pwd-e	Flag of changing password attributes
au-deny	Flag of forbidden web authenticated landing attributes
login	Login authentication authority
vpn	VPN authentication authority
vbr	VPN Branch flag
webauth	Web Authentication authority
ssl-deny	Forbidden sslvpn authenticated landing attributes
bind	Binding flag: 0 - no binding, 1 - single-way binding, 2 - two-way binding
h-pwd	Flag of passwords
idx	Index of the network
ssl-radius	Verification attribute of SSLVPN account.
IP	Configured IP address

1.17 show subs-mab

Use this command to display the status of the subs perception-free mode and bound MAC addresses.

show subs-mab {**all | state**}

Parameter Description

Parameter	Description

N/A	N/A

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide Displays the status of the subs perception-free mode and bound MAC addresses.

Configuration Examples 1: #Display the status of the subs perception-free mode.

```
FS#show subs-mab state
layer23 subs-mab state:On.
```

2: #Display information of the MAC address bound to the subs perception-free authentication.

```
FS#show subs-mab all

Mab current number:1

    00d0.f822.33cc
```

1.18 show vlan-group

Use this command to display VLAN information.

show vlan-group [*name-str*]

Parameter Description

Parameter	Description
name-str	Displays specified VLAN information

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide Displays the VLAN information.

Configuration Examples 1: #Display detailed information of all VLANs.

```
vlan-group                              index vlan_id
root                                    1
tt                                      36028 1,9
```

Field Interpretation

Field	Description
name	Name of the VLAN
index	Index of the VLAN
vlan_id	VID in the VLAN

1.19 subscriber

Use this command to move a subscriber to another parent.

subscriber *str1* **move to parent** *str2*

Parameter Description

Parameter	Description
str1	Name of the subscriber to be moved
str2	Name of the parent network of the moved subscriber

Defaults N/A

Command Mode Privileged EXEC mode

Default level 14

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 child networks.

Configuration Examples

1: #Move the User A originally under root directory to Group 1.

```
FS# subscriber userA move to parent group1
```

Verification Use the **show subscriber brief** command to display whether the layered structure query of the current subscriber is successful.

Prompt Information

1: Cannot find the name of the subscriber to be moved.

```
cannot find the child-subs.
```

2: Cannot find the name of the parent network of the moved child network.

```
cannot find the parent-subs.
```

3: Cannot move to parent of yourself.

```
cannot move to parent of yourself.
```

4: Cannot move the root.

```
cannot move the root.
```

5: Needn't to move the subscriber to its original parent subscriber.

```
the subscriber needn't to be moved.
```

6: Child networks of the non-group parent network cannot be moved.

```
childs of the range-subscriber cannot be moved.
```

7: The parent after changed should be the subscriber group.

```
the parent after changed should be the subscriber group!
```

8: Cannot move to the child of yourself.

```
cann't move to the child of yourself.
```

9: The depth of the subscriber structure is more than 5!

```
the depth of the subscriber moving is more than 5!
```

10: Cannot move the system default subscriber.

```
cannot move the system default subs.
```

Common Errors

1: The depth of subscriber structure after movement surpasses the limitation, which leads to the failed movement.

2: The system default subscriber cannot be moved.

1.20 subscriber allow

Use this command to set the privilege of the subscriber account.

subscriber allow *string* **privilege** { **none** | { [**webauth**] [**vpn**] [**login**] } }

ℹ Use the **no** form of this command to invalidate the privilege set by the command and a newly configured privilege command will cover the original one.

Parameter Description

Parameter	Description
string	Name of the subscriber account
none	Forbids all privileges
webauth	Web authentication authority
vpn	VPN authentication authority
login	Login authentication authority

Defaults

Allows VPN and WEB authentication of subscriber accounts by default.

Command Mode

Global configuration mode

Default level

14

Usage Guide

You can set the privilege of the account by allowing none, one, or two or all of login, VPN and WEB authentication.

ℹ Login authentication currently does not support account authentication under subscriber management.

Configuration Examples

1: #Set VPN and login authorities for "User 1"..

```
FS(config)# subscriber allow User 1 privilege vpn login
```

2: #Set none privilege for "User 1".

```
FS(config)# subscriber allow User 1 privilege none
```

Verification

Use the **show subscriber by-name** *str* command to display whether the login, VPN and webauth flags of a subscriber are **1**, indicating the settings of the privileges.

```
name                                          mac                         dir av-fc av-con vip rel deny pwd-e au-deny login
vpn vbr webauth bind h-pwd idx                ip
xhl                                         0000.0000.0000     0       0        0          0     0     0       0        0           0
1     0     1            2       0         310883589 172.18.3.81
```

Prompt Information

1: Cannot find the subscriber.

```
cannot find this subscriber.
```

2: Cannot set privilege for the system default subscribers.

```
cannot set privi to the system default subs.
```

3: Cannot set privilege for subscriber groups.

```
cannot set privi to subscriber group.
```

Common Errors

1: The depth of network structure after movement surpasses the limitation, which leads to the failed movement.

2: The system default group cannot be moved.

1.21 subscriber export

Use this command to export configuration of subscribers in the current system into an external file.

subscriber export { **txt** | **csv** } *filename*

Parameter Description

Parameter	Description
filename	File name

Defaults

N/A

Command Mode

Privileged EXEC mode

Default level

14

Usage Guide

This command is mainly to export in batches the configuration of subscribers in the current system into an external file.

Configuration

1: #Export subscriber configuration into file “user-info.txt”.

Examples

```
FS# subscriber export txt user-info.txt
```

Verification

Use the commands **show subscriber all** and **show subscriber brief**, and then open the **user-info.txt** to display whether the current configuration is exported into the file.

1.22 subscriber import

Use this command to import a subscriber into the current configuration.

subscriber import { **txt** | **csv** } *filename* [**overwrite**]

Parameter Description

Parameter	**Description**
filename	File name
overwrite	Flag of collision mode

Defaults

N/A

Command Mode

Privileged EXEC mode

Default level

14

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 with ",", and items without content can be blank but with "," remained; 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 file:

/ 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 should be: one record with 6 columns, including parent-sub path, subscriber name password, IP address, MAC address and flag of two-way bind.

In normal mode, subscribers in collision will fail to create the file. In overwrite mode, all subscribers in collision will be eliminated, including collision in name, IP address and MAC address, and then a new network will be created.

Configuration Examples

1: #Import subscriber file “user-info.txt”.

```
FS# subscriber import txt user-info.txt
```

Verification

Use the commands **show subscriber all** and **show subscriber brief** to display whether the current configuration contains the subscriber successfully imported.

1.23 subscriber rename

Use this command to rename subscribers.

subscriber rename *oldname newname*

Parameter Description

Parameter	Description
oldname	Original name of the subscriber
newname	New name of the subscriber

Defaults

N/A

Command Mode

Privileged EXEC mode

Default level

14

Usage Guide

This command is mainly to change the name of a subscriber which will not change other attributes of the subscriber.

Configuration Examples

1: #Rename the subscriber User A the User B.

```
FS# subscriber rename userA userB
```

Verification

Use the **show subscriber by-name** *userB* command to display whether other attributes of the subscriber were changed after rename.

Prompt Information

1: New name already existed.

```
name is conflict with other subscriber.
```

2: Cannot find the subscriber with the old name.

```
cannot find this subscriber
```

3: Cannot rename the system default subscriber.

```
cannot rename the system default subs.
```

1.24 subscriber set

Use this command to set subscriber attributes.

subscriber set *namestr* **attribute** {**avoid-monitor**[**flow-monitor**] | **deny** | **release | vip** | **auth-deny** | **pwd-edit | ssl-auth-deny | ssl-radius-verify**}

Use the **no** form of this command to eliminate special attributes of the subscriber.

no subscriber set *namestr* **attribute** { **avoid-monitor** | **deny** | **release | vip** | **auth-deny** | **pwd-edit | ssl-auth-deny | ssl-radius-verify** }

Parameter Description

Parameter	Description
namestr	User name
avoid-monitor	Avoid-monitor attributes include application identification, content audit and flow control.
flow-monitor	Avoids monitoring but nor flow control
deny	Denies attributes
release	Whitelist attributes, i.e. attribute of eliminating denied subscribers.
vip	VIP attributes
auth-deny	Forbidden landing attribute
pwd-edit	Password changeable attributes
ssl-auth-deny	Forbidden SSLVPN authentication attributes (which can be based on group configuration.)
ssl-radius-verify	Verification-exempted attribute of SSLVPN local account and password.

Defaults Contains no special attribute by default.

Command Mode Global configuration mode

Default level 14

Usage Guide Using avoid-monitor attributes will not enable flow control, content audit and application identification about the subscriber by default, 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 valid only in non-deny mode, and if avoid-monitor attributes and deny attributes are set at the same time, then the deny attributes will be prior.

Whitelist attributes are valid only in deny mode and all subscribers cannot access to Internet, except whitelist attributes of the subscribers are set to "release" when network access deny mode is enabled.

VIP attributes are used for uniform flow control of static users 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 to Internet and the on-line subscribers using this account will be forced to go off line.

PWD-edit attributes are used for setting the authenticated change password attributes of the account, which will only be valid when internal authentication is enabled. By the configuration, the on-line subscribers using this account can change the password by themselves.

SSL-auth-deny attributes are used for setting the forbidden SSLVPN authentication attributes of account (groups). By the configuration, the account itself or accounts in the account group cannot pass the SSLVPN authentication.

The ssl-radius-verify attribute is used to configure the attribute of exempting the SSLVPN local account and password of the account (-group) from verification. With this setting, the SSLVPN local account does not need to go through password verification. When a response times out, the account and password will be verified on the RADIUS server.

Configuration Examples

1: #Configure attributes of avoiding content audit, application identification and flow monitor for "User 1".

```
FS(config)# subscriber set User 1 attribute avoid-monitor flow-monitor
```

2: #Eliminate avoid-monitor attributes of "User 1".

```
FS(config)# no subscriber set User 1 attribute avoid-monitor
```

Verification

Use the **show subscriber by-name** *userB* command to display all messages of the subscriber.

Prompt Information

1: Cannot find the subscriber.

```
cannot find this subscriber.
```

2: Cannot set special attributes for the system default subscribers.

```
cannot set attri to the system default subs.
```

3: Cannot set special attributes for the subscriber group.

```
cannot set attribute to subscriber group.
```

1.25 subscriber static

Use this command to configure a subscriber.

subscriber static name *namestr* **parent** *parstr* [[[[**ip-host** *ip-addr*] [**mac** *mac-addr*] | **ip-subnet** *subnetmask* **|** **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*]

Use the **no** form of the command to disable the function.

no subscriber static name *namestr*

Parameter Description

Parameter	**Description**
namestr	Subscriber name
parstr	Parent path of the subscriber
ip-addr	IP Address
mac-addr	MAC Address
subnet	Start address of IP segment
mask	Mask
start	Start address of IP range

end	End address of IP range
pwd_str	Password **0**: Plain text **6**: md5 text **7**: encrypted text
two-way-bind	Flag of two-way-bind
single-way-bind	Flag of single-way-bind
phone_number	Mobile number.

Defaults VPN_Group, Default_Group and without_auth_user are created by default.

Command Mode Global configuration mode

Default level 14

Usage Guide The IP address of the subscribers must not collide with that of any subscriber except the parent subscriber, and the MAC address of the subscriber must not collide with that of any subscriber.

By IP address, subscribers consist of single IP address subscriber, IP segment subscriber and IP 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 segment, while IP segment subscriber and IP range subscriber can only have MAC address or IP segment. MAC address matching will be prior when both MAC address and IP address are matching.

There is a default subscriber "/", and when layer23 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 subscriber.

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 by two ways. In this way, the account can only use a segment of the IP address or MAC address, which can only be 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 not bound with any IP address or MAC address are not limited by the used IP address or MAC address, while accounts with IP address and MAC address are two-way bound by default.

For internal authentication, IP address will be automatically added to the account, while IP addresses will be added to webauth_root when their on-line accounts are out of the range of the tree.

ⓘ Names of subscribers are exclusive.

Configuration Examples 1: #Configure "User 1" with IP address of "192.168.196.156", whose parent is "User group 1" and the parent of "User group 1" is "All users group".

```
FS(config)# subscriber static name user1 parent /all user-group/user-group1 ip-host 192.168.196.156
```

Verification Use the **show subscriber all** command to display all subscriber information.

Prompt Information

1: Cannot find the subscriber.

```
cannot find this subscriber!
```

2: Cannot delete the default subscriber group

```
cannot delete the default group.
```

3: Parent path errors.

```
Parent string error.
```

4: Configured parent subscriber errors.

```
parent subscriber error.
```

5: Parent subscriber cannot be the have-pwd-subs.

```
parent subscriber cannot be the have-pwd-subs.
```

6: Parent of the have-pwd-subs must be the subscriber group.

```
par of the have-pwd-subs must be the group.
```

7: The name collides with xxx.

```
name conflict with xxx.
```

8: Subscriber group and subscriber cannot exchange.

```
subscriber group and subscriber cannot exchange
```

9: The non-group subscribers with child subscribers cannot be set with passwords.

```
the no-group subs had child-subs cannot set password.
```

10: IP address configuration collides with xxx.

```
ip conflict with xxx.
```

11: IP address configuration collides with single-way-bind xxx.

```
ip conflict with bind-single-way xxx.
```

12: MAC address configuration collides with xxx.

```
mac conflict with xxx.
```

13: MAC address configuration collides with single-way-bind xxx.

```
mac conflict with single-bind xxx.
```

14: IP address errors.

```
ip address error.
```

15: The parent of an IP range subscriber must be a subscriber group.

```
parent of ip range subscriber must be subscriber group.
```

16: IP address or mask errors.

```
ip or mask error
```

17: IP address of the configured IP-RANGE subscriber collides with single-way-bind xxx.

```
IP-RANGE: ip conflict with bind-single-way xxx.
```

18: The length of the phone number is incorrect.

```
the len of phone number is not 11.
```

19: The phone number is invalid.

```
the phone number is illegal.
```

20: The phone number is already in use.

```
the phone number is conflict with xxx.
```

Common Errors

1: Misunderstanding of the concepts of single-way- and two-way-bind.

2: Authentication failure due to account privilege configuration.

1.26 VLAN-group

Use this command to configure VLANs.

vlan-group *name* **vlan** *vid-list*

Use the **no** form of the command to disable the function.

no vlan-group *name*

Parameter Description

Parameter	Description
name	Name of the VLAN
vid-list	VLAN vid

Defaults N/A

Command Mode Global configuration mode

Default level 14

Usage Guide It is recommended that there is no conflict between VLAN IDs of VLANs and VLAN IDs be separated with ",". If a series of VLAN IDs to be configured belongs to the same VLAN, it is recommended to separate start VLAN ID and end VLAN ID with "-" to represent multiple continuous VLAN IDs.

There is a default VLAN "any" by default, and when layer23 classification is enabled, all data flow will match with the default VLAN "any" by default in gateway mode.

In bridge mode, the default match of all data flow will be the corresponding VLAN of Native VLAN in the bridge. If the Native VLAN in the bridge does not have any corresponding VLAN, then data flow will match with the default VLAN "any".

ℹ Name of VLANs must be different, and the identification of VLAN is not available in gateway mode.

Configuration Examples

1: #Configure VLAN "VLAN-group 1", compromising VLAN 1, VLAN 3, VLAN 7, VLAN 8 and VLAN 9.

```
FS(config)# vlan-group vlan-group1 vlan 1,3,7-9
```

Verification Use the **show vlan-group all** command to display all information about the VLAN.

2 APP-IDENTIFY Commands

2.1 app-add

Use this command to add applications to a user-defined group.

app-add *app-name*

Use this command to delete applications from a user-defined group.

app-del *app-name*

Parameter Description

Parameter	Description
app-name	Indicates the name of an application.

Defaults No application is added in a user-defined group by default.

Command Mode Custom group configuration mode

14

Usage Guide Use this command to add applications (including applications and application classes) to a user-defined group.

Configuration Example #Add the game Zhengtu to the user-defined group MYGAME.

```
FS#config
FS(config)#identify-application custom-group MYGAME
FS(config-custom-group)#app-add Zhengtu
```

1. If the application does not exist, the following message is displayed:

```
FS#config
FS(config)#identify-application custom-g
FS(config)#identify-application custom-group aaa
FS(config-custom-group)#app-add no_exit
This application is not exist!
```

2. If the memory is insufficient, the following message is displayed:

```
FS#config
FS(config)#identify-application custom-g
FS(config)#identify-application custom-group instant messaging
not enouth memory!
```

3. If the user-defined group is added to another user-defined group, the following message is displayed:

```
FS#config
FS(config)#identify-application custom-group aaa
FS(config-custom-group)#exit
FS(config)#identify-application custom-group bbb
FS(config-custom-group)#app-add aaa
One custom-group cannot join another custom-group!
```

2.2 app-del

Use this command to delete applications from a user-defined group.

app-del *app-name*

Use this command to recover configurations.

app-add *app-name*

Parameter Description

Parameter	Description
app-name	Indicates the name of an application.

Defaults No application is added in a user-defined group by default.

Command Mode Custom group configuration mode

14

Usage Guide Use this command to delete applications (including applications and application classes) from a user-defined group.

Configuration Example #Delete the game Zhengtu from the user-defined group MYGAME.

```
FS#config
FS(config)#identify-application custom-group MYGAME
FS(config-custom-group)#app-del Zhengtu
```

1. If the application does not exist, the following message is displayed:

```
FS#config
FS(config)#identify-application custom-group aaa
FS(config-custom-group)#app-del bcd
This application doesn't exist!
```

2. If the application is not added to the user-defined group, the following message is displayed:

```
FS#config
FS(config)#identify-application custom-group aaa
FS(config-custom-group)#app-del instant messaging
The application doesn't join the custom-group!
```

2.3 identify-application app-db enable

Use this command to enable application collection.

identify-application app-db enable

Use the **no** form of this command to disable application collection.

no identify-application app-db enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is enabled by default.

Command Mode Global configuration mode

14

Usage Guide Use this command to enable application collection.

Configuration Example #Enable application collection.

```
FS#config
FS(config)#identify-application app-db enable
```

2.4 identify-application block

Use this command to add an application to the blocked application group.

identify-application block *app-name*

Use the **no** form of this command to remove an application from the blocked application group.

no identify-application block *app-name*

Parameter Description

Parameter	Description

app-name	Indicates the name of an application.

Defaults

An application is not added to the blocked application group by default.

Command Mode

Global configuration mode

14

Usage Guide

Use this command to add an application to the blocked application group.

Configuration Example

#Add the application MSN to the blocked application group.

```
FS#config
FS(config)#identify-application block MSN
```

Verification

Run the **show identify-application block** command to display all applications in the blocked application group.

1. If the application has been added into another application group, an error message is displayed. For example, if MSN has been added to the rate-limited application group, the following message is displayed:

```
FS(config)#identify-application block MSN
The application has already been joined Inhibitive_Group!
```

2. If the application does not exist, the following message is displayed:

```
FS(config)#identify-application block XXX
The application does not exist!
```

2.5 identify-application clear key-inhibitive-block-other group

Use this command to clear all the applications in the key application group, rate-limited application group, and blocked application group.

identify-application clear key-inhibitive-block-other group

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

14

Usage Guide

An application can be added to one of the following application groups: key application group, rate-limited application group, and blocked application group. The application cannot be added to two application groups at the same time. Use this command to delete all the applications in the key application group, rate-limited application group, and blocked application group.

Configuration Example

#Clear all the applications in the key application group, rate-limited application group, and blocked application group.

```
FS#config
FS(config)# identify-application clear key-inhibitive-block-other group
```

Verification

Run the **show identify-application key, show identify-application inhibitive, show identify-application-block, and show identify-application other** commands to display all the applications in the key application group, rate-limited application group, blocked application group, and Other application group.

2.6 identify-application custom name

Use this command to configure a rule.

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* **} } } }**

Use the **no** form of this command to remove an application from the blocked application group.

no 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

Parameter	Description
software-name	Indicates the name of an application.
class-name	Indicates an application class name.
sport-low	Indicates a start source port. The value range is 0 to 65,535 or the value can be **any**.
sport-high	Indicates an end source port. The value range is 0 to 65,535 or the value can be **any**.
dport-low	Indicates a start destination port. The value range is 0 to 65,535 or the value can be **any**.
dport-high	Indicates an end destination port. The value range is 0 to 65,535 or the value can be **any**.
sip-low	Specifies a start source IP address.

sip-high	Specifies an end source IP address.
dip-low	Specifies a start destination IP address.
dip-high	Specifies an end destination IP address.

Defaults No user-defined rule is available by default.

Command Mode Global configuration mode

14

Usage Guide Use this command to configure a rule.

User-defined applications fall into the following types:

1. Protocol type and source and destination ports
2. Protocol type, source IP address, and source port
3. Protocol type and source and destination IP addresses
4. 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 Example #Configure a rule, and set the application class to a user-defined group, application name to Xunlei Games, source port range to 1–10, destination port range to 1–100, and protocol type to TCP.

```
FS#config
FS(config)#identify-application custom name Xunlei Game class user-defined game tcp sport 1 10 dport 1 100
```

#Configure a rule, and set the application class to myp2p, application name to myxunlei, source port to any, destination port to 200, and protocol type to UDP.

```
FS#config
FS(config)#identify-application custom name myxunlei class myp2p udp sport any any dport 200 200
```

#Configure a rule, and set the application class to myqq, application name to im in the signatures database, source port to 111, destination port to 2020, and protocol type to UDP.

```
FS#config
FS(config)#identify-application custom name myqq class im udp sport 111 111 dport 2020 2020
```

Verification Run the **show identify-application custom-rule** command to display all user-defined rules.

1. If the number of IP addresses is greater than 32, the following message is displayed:

```
FS(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18. 2.255 dport 2
2
High ip address must be larger than low ip address,and the range of ip address can not be larger than 32!
```

2. If the IP address or port cannot be set to any, the following message is displayed:

```
FS(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18. 2.255 dport
any any
It's not allow for either dst ip address or dst port number are "any"!
```

3. If the IP address or port conflicts with another, the following message is displayed:

```
FS(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18. 1.30 dport 2 2
FS(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.25 172.18. 1.35 dport 2 2
Port or ip has already used!
```

4. If the IP address or port conflicts with another, the following message is displayed:

```
FS#show identify-application custom-rule
TYPE NAME                          CLASS                              SPL    SPH    DPL    DPH
SIPL              SIPH              DIPL              DIPH
---- -------------------------- ------------------------------- ----- ----- ----- ----- --------------- --------------- --------------- ---------------
TCP   rule1                         TC_AD_KEY                        any    any     2      2
any               any               172.18.1.20       172.18.1.30
TCP   rule2                         TC_AD_KEY                        any    any     3     20
any               any               172.18.1.25       172.18.1.26
TCP   rule3                         Database                         any    any    25     30
any               any               172.18.1.25       172.18.1.25
TCP   rule3                         Database                         any    any    35     40
any               any               172.18.1.25       172.18.1.29
TCP   rule3                         Database                         any    any    45     50
```

```
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     55      60
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     65      70
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     72      72
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     74      74
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     76      76
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     78      78
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     80      80
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     82      82
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     84      84
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     86      86
any             any             172.18.1.25     172.18.1.29
TCP    rule3                       Database                               any     any     88      88
any             any             172.18.1.25     172.18.1.29
FS(config)# identify-application custom name rule3 class Database tcp dip 172.18.1.25 172.18.1. 29 dport 90 90
The same IP associated with different port cannot exceed 16
```

2.7 identify-application custom-group

Use this command to define a group.

identify-application custom-group *group-name*

Use the **no** form of this command to delete a user-defined group.

no identify-application custom-group *group-name*

Parameter Description

Parameter	Description
group-name	Indicates the name of an application group.

Defaults No application group is self-defined by default.

Command Mode

Global configuration mode

14

Usage Guide

Use this command to define a group.

A maximum of 100 classes of application groups can be defined.

After the command is run, enter the custom group configuration mode.

Configuration Example

#Add an application group MYGAME. The level of this application group is the same as that of the key application group and rate-limited application group.

```
FS#config
FS(config)#identify-application custom-group MYGAME
FS(config-custom-group)#
```

1. If the user-defined group to be deleted does not exist, the following message is displayed:

```
FS(config)#no identify-application custom-group abc
The custom-group doesn't exist!
```

2. If the name of the user-defined group conflicts with a system application, the following message is displayed:

```
FS(config)#id custom-group instant messaging
The application name is conflict with application in system!
```

3. If the number of application groups is greater than a threshold, the following message is displayed:

```
FS(config)#id custom-group group101
The number of custom-group cannot be more than 100!
```

2.8 identify-application dfi enable

Use this command to enable DFI to identify P2P download flows and voice flows.

identify-application dfi enable

Use the **no** form of this command to disable DFI.

no identify-application dfi enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default, and it can be enabled separately.

Command Mode

Global configuration mode

14

Usage Guide

Use this command to enable DFI to identify P2P download flows and voice flows.

Configuration Example

#Enable DFI to identify P2P download flows and voice flows.

```
FS#config
FS(config)#identify-application dfi enable
```

Verification

Run the **show running-config** command to display the function status. If the function is disabled, the following message is displayed:

```
identify-application dfi enable
```

2.9 identify-application dpi enable

Use this command to enable DPI.

identify-application dpi enable

Use the **no** form of this command to disable DPI.

no identify-application dpi enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

DPI is enabled by default provided that APP-IDENTIFY is enabled.

Command Mode

Global configuration mode

14

Usage Guide

Use this command to enable DPI.

Configuration Example

#Enable DPI.

```
FS#config
FS(config)#identify-application dpi enable
```

Verification

Run the **show running-config** command to display the function status. If the function is disabled, the following message is displayed:

```
no identify-application dpi enable
```

2.10 identify-application enable

Use this command to enable APP-IDENTIFY globally.

identify-application enable

Use the **no** form of this command to disable APP-IDENTIFY globally.

no identify-application enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

14

Usage Guide Use this command to enable APP-IDENTIFY globally.

Configuration Example #Enable APP-IDENTIFY.

```
FS#config
FS(config)#identify-application enable
```

Verification Run the **show identify-application enable** command to display the function status.

2.11 identify-application inhibitive

Use this command to add an application to the rate-limited application group.

identify-application inhibitive *app-name*

Use the **no** form of this command to remove an application from the rate-limited application group.

no identify-application inhibitive *app-name*

Parameter Description

Parameter	Description
app-name	Indicates the name of an application.

Defaults An application is not added to the rate-limited application group by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to add an application to the rate-limited application group.

Configuration Example

#Add the application MSN to the rate-limited application group.

```
FS#config
FS(config)#identify-application inhibitive MSN
```

Verification

Run the **show identify-application inhibitive** command to display all applications in the rate-limited application group.

1. If the application has been added into another application group, an error message is displayed. For example, if MSN has been added to the blocked application group, the following message is displayed:

```
FS(config)#identify-application inhibitive MSN
The application has already been joined Block_Group!
```

2. If the application does not exist, the following message is displayed:

```
FS(config)#identify-application inhibitive XXX
The application does not exist!
```

2.12 identify-application key

Use this command to add an application to the key application group.

identify-application key *app-name*

Use the **no** form of this command to remove an application from the key application group.

no identify-application key *app-name*

Parameter Description

Parameter	Description
app-name	Indicates the name of an application.

Defaults

An application is not added to the key application group by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to add an application to the key application group.

Configuration Example

#Add the application MSN to the key application group.

```
FS#config
FS(config)#identify-application key MSN
```

Verification Run the **show identify-application key** command to display all applications in the key application group.

1. If the application has been added into another application group, an error message is displayed. For example, if MSN has been added to the blocked application group, the following message is displayed:

```
FS(config)#identify-application key MSN
The application has already been joined Block_Group!
```

2. If the application does not exist, the following message is displayed:

```
FS(config)#identify-application key XXX
The application does not exist!
```

2.13 identify-application len-seq enable

Use this command to enable length sequence identification.

identify-application len-seq enable

Use the **no** form of this command to disable length sequence identification.

no identify-application len-seq enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Length sequence identification is enabled by default provided that APP-IDENTIFY is enabled.

Command Mode Global configuration mode

Usage Guide Use this command to enable length sequence identification.

Configuration Example #Enable length sequence identification.

```
FS#config
FS(config)#identify-application len-seq enable
```

Verification Run the **show running-config** command to display the function status. If the function is disabled, the following message is displayed:

```
no identify-application len-seq enable
```

2.14 identify-application other

Use this command to add an application to the Other application group.

identify-application other *app-name*

Use the **no** form of this command to remove an application from the Other application group.

no identify-application other *app-name*

Parameter Description

Parameter	Description
app-name	Indicates the name of an application.

Defaults An application is added to the Other application group by default.

Command Mode Global configuration mode

Usage Guide Use this command to add an application to the Other application group.

Configuration Example #Add the application MSN to the Other application group.

```
FS#config
FS(config)#identify-application other MSN
```

Verification Run the **show identify-application other** command to display all applications in the Other application group.

If the application does not exist, the following message is displayed:

```
FS(config)#identify-application other XXX
The application does not exist!
```

2.15 identify-application proto-detect enable

Use this command to enable detective identification.

identify-application proto-detect enable

Use the **no** form of this command to disable detective identification.

no identify-application proto-detect enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Detective identification is enabled by default provided that APP-IDENTIFY is enabled.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable detective identification.

Configuration Example

#Enable detective identification.

```
FS#config
FS(config)# identify-application proto-detect enable
```

Verification

Run the **show running-config** command to display the function status. If the function is disabled, the following message is displayed:

```
no identify-application proto-expect enable
```

2.16 identify-application proto-expect enable

Use this command to enable predictive identification.

identify-application proto-expect enable

Use the **no** form of this command to disable predictive identification.

no identify-application proto-expect enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Predictive identification is enabled by default provided that APP-IDENTIFY is enabled.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable predictive identification.

Configuration Example

#Enable predictive identification.

```
FS#config
FS(config)# identify-application proto-expect enable
```

Verification

Run the **show running-config** command to display the function status. If the function is disabled, the following message is displayed:

```
no identify-application proto-expect enable
```

2.17 identify-application proto-expect timeout

Use this command to configure aging time of protocol information.

identify-application proto-expect timeout *time-seconds*

Use the **no** form of this command to cancel aging time of protocol information.

no identify-application proto-expect timeout

Parameter Description

Parameter	Description
time-seconds	Indicates the aging time in seconds. The value range is 10 to 3,600.

Defaults The aging time is 60 seconds by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure aging time of protocol information.

Configuration Example #Set the aging time of protocol information to three minutes.

```
FS#config
FS(config)# identify-application proto-expect timeout 180
```

Verification Run the **show running-config** command to display the configuration result. If aging time is configured, the following message is displayed:

```
identify-application proto-expect timeout 180
```

2.18 identify-application signature update

Use this command to upgrade the signatures database.

identify-application signature update

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the gateway automatically upgrades the signatures database within one minute after the gateway is started.

Command Mode Global configuration mode

Usage Guide Use this command to upgrade the signatures database.

Configuration Example

#Download the latest signatures database from the URL provided on the Web upgrade interface.

#Decompress the package, and download the signatures database to the gateway over TFTP.

```
FS#copy tftp://172.18.3.11/app_signature.upd flash:app_signature.upd
Accessing tftp://172.18.3.11/app_signature.upd...
!!!!!!!!!!!!!!!!
Transmission finished, file length 242952     bytes.


Download file [app_signature.upd] to file system is OK.
FS#run-system-shell
~ # cp /data/app_signature.upd /sbin/signature/app_tmp/
~ # exit
FS#
```

#Upgrade the signatures database.

```
FS#config
FS(config)# identify-application signature update
```

Verification Run the **show identify-application version** command to display the version number of the signatures database.

2.19 show identify-application

Use this command to display the application tree information.

show identify-application

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide Use this command to display the current application tree information.

Configuration Example

#Display the application tree information.

```
FS#show identify-application
any 255-4095-63-48
    Instant messaging 1-0-0-0
        Ali Wangwang 1-1-0-0
        MSN 1-6-0-0
            MSN-CHAT 1-6-1-0
            MSN-AUDIO 1-6-2-0
            MSN-FILE 1-6-3-0
            MSN-video 1-6-4-0
            MSN-login 1-6-5-0
        Tencent QQ 1-7-0-0
            QQ-CHAT 1-7-1-0
            QQ-voice 1-7-2-0
            QQ-file transfer 1-7-3-0
            QQ-file sharing 1-7-4-0
            QQ-video 1-7-5-0
            QQ-login 1-7-14-0
        WEBIM 1-9-0-0
            MSN-WEBIM 1-9-1-0
            YAHOO-WEBIM 1-9-2-0
            AIM 1-9-3-0
        NetEase Popo 1-12-0-0
        Fetion 1-14-0-0
    VoIP 2-0-0-0
        SKYPE 2-7-0-0
        h232 protocol stack 2-12-0-0
            H323-HOSTCALLSC 2-12-4-0
            CALL-SIG-TRANS 2-12-5-0
            RTCP 2-12-6-0
            RTP 2-12-7-0
           IMTC-MCS 2-12-10-0
```

2.20 show identify-application block

Use this command to display the applications or application classes that are added to the blocked application group.

show identify-application block

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the applications or application classes that are added to the blocked application group.

Configuration Example

#Display the applications that are added to the blocked application group.

```
FS# show identity-application block
Stock
Baidu Download
Xunlei
```

2.21 show identify-application class

Use this command to display application class information.

show identify-application class [*class-name*]

Parameter Description

Parameter	**Description**
class-name	Indicates an application class.

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display application class information or applications of a class.

Configuration Example

#Display application classes.

```
FS# show identify-application class
Instant messaging 1-0-0-0
VoIP 2-0-0-0
Online game 3-0-0-0
Video streaming 4-0-0-0
P2P 5-0-0-0
Stock 6-0-0-0
Web application 7-0-0-0
HTTP game 38-0-0-0
Internet file transfer 8-0-0-0
Email 9-0-0-0
Database 10-0-0-0
```

```
Network management protocol 11-0-0-0

Routing protocol 12-0-0-0

Security protocol 13-0-0-0

VPN application 14-0-0-0

Remote access protocol 15-0-0-0

Software update 17-0-0-0

HTTP video 18-0-0-0

Online banking 19-0-0-0

Network disk 20-0-0-0

Instant messaging_MOBILE 21-0-0-0

Video|movie & music_MOBILE 22-0-0-0

Downloader_MOBILE 23-0-0-0

Game_MOBILE 24-0-0-0
```

#Display applications of a class.

```
FS# show identify-application class Internet file transfer

FTP 8-4-0-0

HTTPS 8-7-0-0

NNTP 8-12-0-0

TFTP 8-16-0-0

IXIA 8-17-0-0

SVN 8-18-0-0

SMB 8-21-0-0

HFS 8-22-0-0
```

2.22 show identify-application custom-group

Use this command to display application group information.

show identify-application custom-group

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display all application group information.

Configuration Example

#Display application group information.

```
FS# show identify-application custom-group
system-group: Key_Group
system-group: Unkey_Group
system-group: Block_Group
    application: MSN (group)
system-group: Other_Group
    application: instant messaging (group)
    application: VoIP (group)
    application: online game (group)
    application: video streaming (group)
    application: P2P (group)
    application: stock (group)
    application: web application (group)
    application: HTTP game (group)
    application: Internet file transfer (group)
    application: email (group)
    application: database (group)
    application: network management protocol (group)
    application: routing protocol (group)
    application: security protocol (group)
    application: VPN application (group)
    application: remote access protocol (group)
    application: software update (group)
    application: HTTP video (group)
    application: online banking (group)
    application: network disk (group)
    application: instant messaging_MOBILE (group)
    application: video|movie & music_MOBILE (group)
    application: downloader_MOBILE (group)
    application: game_MOBILE (group)
    application: social network_MOBILE (group)
    application: online banking_MOBILE (group)
    application: WEB_MOBILE (group)
    application: other_MOBILE (group)
    application: online purchase_MOBILE (group)
    application: securities_MOBILE (group)
    application: online payment|online banking_MOBILE (group)
    application: microblog (group)
    application: office OA (group)
    application: video conference (group)
    application: HTTP download (group)
    application: HTTP upload (group)
    application: RFC (group)
    application: ICMP-DETAIL (group)
    application: IP-RAW (group)
    application: IP protocol group (group)
    application: TC_AD_KEY (group)
custom-group: TC_AD_Key
    application: web application (group)
    application: HTTP download (group)
    application: P2P-HTTP download
    application: downloader_MOBILE (group)
custom-group: route~route
    application: web application (group)
    application: HTTP download (group)
    application: HTTP upload (group)
custom-group: 1~route
    application: HTTP download (group)
    application: HTTP upload (group)
```

2.23 show identify-application custom-rule

Use this command to display the user-defined application rules.

show identify-application custom- rule

Parameter Description

Parameter	**Description**

N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display all user-defined application rules.

Configuration Example

#Display application group information.

```
FS# show identify-application custom- rule
TYPE NAME                              CLASS                              SPL    SPH    DPL    DPH
SIPL                SIPH                DIPL                DIPH
---- -------------------------- ------------------------------ ----- ----- ----- ----- --------------- --------------- --------------- ---------------
TCP   rule1                            TC_AD_KEY                            any    any    2      2
any                 any                 172.18.1.20         172.18.1.30
TCP   rule2                            TC_AD_KEY                            any    any    3      20
any                 any                 172.18.1.25         172.18.1.26
TCP   rule3                            Database                             any    any    25     30
any                 any                 172.18.1.25         172.18.1.25
TCP   rule3                            Database                             any    any    35     40
any                 any                 172.18.1.25         172.18.1.29
TCP   rule3                            Database                             any    any    45     50
any                 any                 172.18.1.25         172.18.1.29
TCP   rule3                            Database                             any    any    55     60
any                 any                 172.18.1.25         172.18.1.29
TCP   rule3                            Database                             any    any    65     70
any                 any                 172.18.1.25         172.18.1.29
TCP   rule3                            Database                             any    any    72     72
any                 any                 172.18.1.25         172.18.1.29
TCP   rule3                            Database                             any    any    74     74
any                 any                 172.18.1.25         172.18.1.29
```

Field description:

Field	Description
TYPE	Indicates protocol information.
NAME	Indicates a rule name.
CLASS	Indicates a class of applications to which the rules apply.
SPL	Specifies a start source port.
SPH	Specifies an end source port.
DPL	Specifies a start destination port.
DPH	Specifies an end destination port.

SIPL	Indicates a start source IP address.
SIPH	Indicates an end source IP address.
DIPL	Indicates a start destination IP address.
DIPH	Indicates an end destination IP address.

2.24 show identify-application dfi enable

Use this command to display DFI.

show identify-application dfi enable

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display DFI.

Configuration Example

#Display DFI.

```
FS# show identify-application dfi enable
dfi enable!
```

2.25 show identify-application enable

Use this command to display the status of the application identification function.

show identify-application enable

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the status of the application identification function.

Configuration Example

#Display the status of the application identification function.

```
FS# show identify-application enable
On
```

2.26 show identify-application group-state

Use this command to display the group mode.

show identify-application group-state

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display current group mode.

Configuration Example

#Display application class information.

```
FS#show identity-application group-state
app group state: on
```

Field description:

Field	Description
app group state	Specifies a group mode. If the value is **on**, current applications are classified into the key application group, rate-limited application group, or IP group.

2.27 show identify-application inhibitive

Use this command to display the applications or application classes that are added to the rate-limited application group.

show identify-application inhibitive

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the applications or application classes that are added to the rate-limited application group.

Configuration Example

#Display the applications in the rate-limited application group.

```
FS# show identity-application inhibitive
Stock
```

```
Baidu Download
Xunlei
```

2.28 show identify-application key

Use this command to display the applications or application classes that are added to the key application group.

show identify-application key

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the applications or application classes that are added to the key application group.

Configuration Example

#Display the applications in the key application group.

```
FS# show identity-application key
MSN
QQ
```

2.29 show identify-application other

Use this command to display the applications or application classes that are added to the Other application group.

show identify-application other

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the applications or application classes that are added to the Other application group.

Configuration Example

#Display the applications in the Other application group.

```
FS# show identity-application other
MSN
QQ
```

2.30 show identify-application proto-detect enable

Use this command to display the detective protocol information.

show identify-application proto-detect enable

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the current detective protocol information.

Configuration Example

#Display the detective protocol information.

```
FS#show identify-application proto-detect enable
proto-detect is on
```

2.31 show identify-application proto-expect enable

Use this command to display the predictive protocol information.

show identify-application proto-expect enable

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the current predictive protocol information.

Configuration Example

#Display the predictive protocol information.

```
FS#show identify-application proto-expect enable
Proto-expect is enable
Proto-expect app_db is unable
Proto-expect timeout is not set[0s]
```

2.32 show identify-application version

Use this command to display the version number of the signatures database.

show identify-application version

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the current version number of the signatures database.

Configuration Example

#Display the current version number of the signatures database.

```
FS# show identify-application version

Version:2013.06.10.13.06.10(V2.0)
```

Field description:

Field	Description
Version	Indicates a version number.

3 APP-ROUTE Commands

3.1 app route app-name

Use this command to configure application routing policies.

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***] [**static-route**] [**description** ***description-name***]

Use the **no** form of this command to delete application routing policies.

no app route priority-num *priority-num*

Use this command to restore the default configuration.

default app route priority-num *priority-num*

Parameter Description

Parameter	**Description**
priority-num	Indicates an application route priority that identifies a policy uniquely. The value range is 1 to 10,000.
protocol-num	Indicates an IP protocol number which is specified by APP-ROUTE. The value range is 1 to 255.
s-begin	Indicates a start source port number. The value range is 1 to 65,535.
s-end	Indicates an end source port number. The value range is 1 to 65,535. This parameter is optional. The value of this parameter must be greater than that of the start source port number ***s-begin***.
d-begin	Indicates a start destination port number. The value range is 1 to 65,535.
d-end	Indicates an end destination port number. The value range is 1 to 65,535. This parameter is optional. The value of this parameter must be greater than that of the start destination port number ***d-begin***.
app-name	Indicates an application name. This parameter can be set to the name of an application class, application software, application software sub class, or group, or set to **any**.
sip-group-number	Indicates a source IP group ID. Configure an IP group and a source IP address for the group before selecting a route. The value range is 1 to 1,000.
dip-group-number	Indicates a destination IP group ID. Configure an IP group and a destination IP address for the group before selecting a route. The value range is 1 to 1,000.
url-group-name	Indicates a URL group name. The group can be a system group (for example, video~sys), user-defined group, or set to **any**.
dest-ip-address	Specifies the IP address of a DNS server that parses a URL of a group (if any).
interface-name	Specifies an interface name.

group-name	Specifies 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 the track object associated with a rule.
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.
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.
description-name	Indicates the remarks of an application routing policy. For example, sys indicates that the quick guide is automatically generated.

Defaults No application routing policy is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure an application route so that data flows of specified applications can be forwarded through the specified egress interface. Application types fall into application class, application software, application software sub class, and application group. APP-ROUTE supports applications with an identifiable initial packet of data flows. With the application identification capability improved, the types of applications supported by APP-ROUTE will be increasingly diversified. For details, refer to the APP-IDENTIFY configuration guide.

APP-ROUTE supports WAN interfaces and WAN interface groups. Generally, one type of applications supports 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, the following conditions must be met:

APP-ROUTE is enabled.

The time specified by the time range parameter arrives.

At least one interface is in the UP state.

Different types of applications are available and support initial packet identification.

There are objects in the URL group.

The tract state is valid.

Configuration Example #Configure application routing based on the egress interface.

```
FS(config)# app route priority-num 2 P2P application software interface GigabitEthernet 0/4 time-range any
```

#Configure application routing based on the egress interface group.

```
FS(config)# app route priority-num 3 rate-limited traffic~route interface-group intf_group
```

#Configure application routing based on the time range.

```
FS(config)# app route priority-num 3 rate-limited traffic~route interface-group intf_group time-range on-work
```

#Configure application routing based on the IP group.

(1). By specifying a source IP group:

```
FS(config)# app route priority-num 2 any sip-group 1 interface-group intf_group time-range any
```

(2). By specifying a destination IP group:

```
FS(config)# app route priority-num 2 any dip-group 2 interface-group intf_group time-range any
```

(3). By specifying a source IP group and a destination IP group:

```
FS(config)# app route priority-num 2 any sip-group 1 dip-group 2 interface-group intf_group time-range any
```

#Configure application routing based on the URL group.

(1). Without a DNS server for URL parsing specified:

```
FS(config)# app route priority-num 2 any url-group QQ netbar interface GigabitEthernet 0/3 time-range any
```

(2). With a DNS server for URL parsing specified:

```
FS(config)# app route priority-num 2 any url-group google change-dest 8.8.8.8 interface GigabitEthernet 0/3
time-range any
```

#Configure application routing based on the track function.

```
FS(config)# app route priority-num 2 any url-group google change-dest 8.8.8.8 interface GigabitEthernet 0/3
time-range any track 1
```

#Configure application routing based on the protocol number or port number.

```
FS(config)# app route priority-num 2 any protocol tcp sport 1 1000 dport 80 interface GigabitEthernet 0/3 time-range
any
```

Verification

1. Run the **show app route** command to display the configuration and validation information of APP-ROUTE.
2. Run the **show app route statistics** command to display the statistical information of APP-ROUTE.
3. Run the **show app route priority-num 2 session** command to display the session information with priority ID being 1.

3.2 app route priority-num priority-number priority

Use this command to configure priorities of application routes.

app route priority-num *priority-number* priority { **increase** | **decrease** } [*1-1999*]

Parameter Description

Parameter	Description
priority-num	Indicates an application route priority that identifies a policy uniquely. The value range is 1 to 10,000.
[*1-1999*]	Indicates a priority interval. If the required value exceeds this value range, the parameter is automatically adjusted to the maximum value.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

The priorities of application routes are related to the configuration sequence. The application route configured later prevails over the application route configured earlier. Priorities can be specified as well. A greater priority value indicates a higher priority.
Use this command to change the priorities of the application routes.

Configuration Example

#Increase the priority of an application routing policy by 1. The value 1 is relative. For example, if the priority of one policy is 20, and the priority of the other policy is 40, increasing priority 20 by 1 gets priority 40, and the original priority 40 decreases to 20.

```
FS(config)# app route priority-num 20 P2P application software priority increase 1
```

2. Decrease the priority of an application routing policy by 1. The rule is the same as that for priority increase.

```
FS(config)# app route priority-num 40 P2P application software priority decrease 1
```

Verification

Run the **show app route** command to display the configuration information of APP-ROUTE.

3.3 app route enable

Use this command to enable APP-ROUTE.
app route enable

Use the **no** form of this command to disable APP-ROUTE.
no app route enable

Use this command to restore the default configuration.
default app route enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

APP-ROUTE is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable APP-ROUTE. Configured application routing policies can be validated only after APP-ROUTE is enabled.

Configuration

#Enable APP-ROUTE.

Example

```
FS(config)# app route enable
```

#Disable APP-ROUTE.

```
FS(config)#no app route enable
```

Verification Run the **show app route** command to display the status of APP-ROUTE.

3.4 app route mode new-flow

Use this command to validate application routing policies for new connections.

app route mode new-flow

Use the **no** form of this command to validate application routing policies for all connections.

no app route mode new-flow

Use this command to restore the default configuration.

default app route mode new-flow

Parameter Description

Parameter	Description
N/A	N/A

Defaults Defaults vary with gateways of different models.

Command Mode Global configuration mode

Usage Guide Use this command to validate application routing policies for new connections. In this case, a change to the application routing policies will not affect traffic that have been routed, namely, the old traffic. After this function is disabled, a change to the application routing policies takes effects immediately to all traffic.

Configuration Example

#Validate application routing policies for new connections.

```
FS# app route mode new-flow
```

#Validate application routing policies for all connections.

```
FS# no app route mode new-flow
```

Verification Run the **show run** | **include app route** command to display the status of APP-ROUTE.

3.5 interface-group

Use this command to configure an interface group.

interface-group interface-group-name

Use the **no** form of this command to delete an interface group.

no interface-group *interface-group-name*

Use this command to restore the default configuration.

default interface-group *interface-group-name*

Parameter Description

Parameter	Description
interface-group-name	Indicates an interface group name.

Defaults No interface group is configured by default.

Command Mode Global configuration mode

Usage Guide An interface group can contain multiple egress interfaces of APP-ROUTE. If the egress interfaces of APP-ROUTE are specified as an interface group, traffic that hits the corresponding application routing policy will be distributed to the interfaces of the group.

Configuration Example #Configure an interface group.

```
FS(config)# interface-group intf-grp
```

Verification Run the **show interface-group** command to display the configuration information of the interface group.

3.6 interface-member

Use this command to configure members for an interface group.

interface-member *interface-name* [**weight** *weight-number*]

Use the **no** form of this command to delete members from an interface group.

no interface-member *interface-name*

Use this command to restore the default configuration.

default interface-member *interface-name*

Parameter Description

Parameter	Description
interface-name	Indicates an interface name.
weight-number	Specifies a weight value of interfaces. The value range is

	1 to 40,000,000 in kbps.

Defaults

No member is not configured for an interface group by default.

An interface group contains no more than 32 members, and they must be non-LAN egress interfaces.

Command Mode

Interface group configuration mode

Usage Guide

Use this command to add interfaces to an 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.

This command supports weight values of user-defined interfaces. The weight values are downlink bandwidth in kbps of the interfaces by default.

3.7 load-balance policy

Use this command to configure policies for an interface group.

load-balance policy { **bandwidth** | **load** }

Use the **no** form of this command to restore default policies of an interface group.

no load-balance policy

Use this command to restore the default configuration.

default load-balance policy

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults

Bandwidth-based policies are used by default.

Command Mode

Interface group configuration mode

Usage Guide

APP-ROUTE distributes and processes traffic of new data flows. If a bandwidth-based policy is used, APP-ROUTE balances the traffic of the data flows according to the bandwidth of different egress interfaces in a group or the weight values defined by users for the interfaces. If a load-based policy is used, APP-ROUTE balances the traffic of the data flows according to the load of different egress interfaces in a group.

Configuration Example

#Configure a bandwidth-based policy for the interface group.

```
FS(config-intf-group)#load-balance policy bandwidth
```

#Configure a load-based policy for the interface group.

```
FS(config-intf-group)#load-balance policy load
```

3.8 nexthop

Use this command to configure the interface gateway function.

nexthop *ip-address*

Use the **no** form of this command to cancel the interface gateway function.

no nexthop

Use this command to restore the default configuration.

default nexthop

Parameter Description

Parameter	**Description**
ip-address	Specifies an IP address.

Defaults No gateway information is configured by default.

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.

Configuration Example #Configure the interface gateway function.

```
FS(config-if-GigabitEthernet 0/1)#nexthop 2.2.2.2
```

#Cancel the interface gateway function.

```
FS(config-if-GigabitEthernet 0/1)#no nexthop
```

Verification Run the **show run interface gigabitEthernet 0/1** command to display the next-hop information of the interface.

3.9 show app route

Use this command to display the configuration information of APP-ROUTE.

show app route [**statistics** | **priority-num** *priority-num* **session** [**ipv6**]]

Parameter Description

Parameter	**Description**

priority-num	Indicates an application route priority that identifies a policy uniquely. The value range is 1 to 10,000.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

14

Usage Guide

Use the **show app route** command to display status information of configured application routes. The arrangement sequence of the application routes indicates the priorities of the application routes. The topmost application route has the highest priority.

Use the **show app route statistics** command to display the general statistical information of APP-ROUTE.

Use the **show app route priority-num** *priority-num* **session** command to display IPv4 session information of a specified application route.

Use the **show app route priority-num** *priority-num* session **ipv6** command to display IPv6 session information of a specified application route.

Configuration Example

#Display the configuration information of APP-ROUTE.

```
FS(config)#show app route
CLASS                                                         SRC-GRP          DST-GRP(URL)
INTERFACE(GROUP)                TIME-RANGE                STATE
--------------------------------      ----------      --------------------------------------------------      ------------------------------
------------------------- ----------
any                                                   any              2(QQ  netbar;:  114.114.114.114)
GigabitEthernet 0/4              any                        Inactive
any                                                             1                              any
test(group)                      any                        Inactive
HTTP                                                            any                            any
GigabitEthernet 0/3              any                        Active
```

Field description:

Field	Description
CLASS	Indicates the name of a type of applications (application group, application class, application software, or application software sub class) for which application routes have been configured.
SRC-GRP	Indicates the ID of a source IP group. The value **any** indicates no configuration.
DST-GRP(URL)	Indicates the ID of a destination IP group. The value **any** indicates no configuration. The content in the brackets indicates a URL of the group, which shows the IP address of the DNS server.
INTERFACE(GRPUP)	Indicates an interface name or interface group name.

TIME-RANGE	Indicates a time range.
STATE	Specifies the state of an application routing policy.

#Display the statistical information of APP-ROUTE.

```
FS(config)#show app route statistics
CLASS                                                             SRC-GRP          DST-GRP(URL)
INTERFACE(GROUP)                  Flows
------------------------------- ---------- ------------------------------------------------- ------------------------------ ----------
any                                                    any                2(QQ  cybercafe;114.114.114.114)
GigabitEthernet 0/4                 0|0
any                                                                 1                             any
test(group)                           0|0
HTTP    Protocol                                                    any                           any
GigabitEthernet 0/3                 0|0
FS(config)#
```

Field description:

Field	Description
CLASS	Indicates the name of a type of applications (application group, application class, application software, or application software sub class) for which application routes have been configured.
SRC-GRP	Indicates the ID of a source IP group. The value **any** indicates no configuration.
DST-GRP(URL)	Indicates the ID of a destination IP group. The value **any** indicates no configuration. The content in the brackets indicates a URL of the group, which shows the IP address of the DNS server.
INTERFACE(GRPUP)	Indicates an interface name or interface group name.
Flows	Indicates the number of IPv4/IPv6 connections for an application routing policy. IPv4 and IPv6 connection numbers are separated by "|".

#Display the session information.

```
FS#show app route priority-num 1112 session
SIP:PORT                    DIP:PORT                    PRO-NUM    INTF           SUM DATA(byte)
---------------------- ---------------------- -------- ---------- ---------------------------------------
192.169.255.100:6007     14.17.41.174:80         6           Gi0/3        368/1001
192.169.255.100:6006     14.17.41.174:80         6           Gi0/3        446/6722
192.169.255.100:6006     14.17.41.174:80         6           Gi0/3        368/1452
```

```
FS#show app route priority-num 1112 session ipv6

SIP:PORT                                                                    DIP:PORT
PRO-NUM    INTF             SUM DATA(byte)

----------------------                                                ----------------------
-------- ---------- ----------------------------------------

2001:250:6803:f300::90:2:1                                            2001::12:32768
58             Gi0/7           40/0
```

Field description:

Field	Description
SIP	Indicates a source IP address.
SPORT	Indicates a source port.
DIP	Indicates a destination IP address.
DPORT	Indicates a destination port.
PRO-NUM	Indicates a protocol number.
INTF	Indicates an interface name.
SUM DATA(byte)	Indicates the total traffic amount of a session, including download and upload statistics.

3.10 show interface-group

Use this command to display the configuration information of an interface group.

show interface-group

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to display the configuration information of all interface groups.

Configuration Example

#Display the configuration information of interface groups.

```
FS #show interface-group

------------------------------------------------------------

GROUP-NAME: intf_group

INTERFACE INCLUDED: di1,di2,di3

POLICY: load

STATE: UP
```

Field description:

Field	Description

GROUP-NAME	Indicates an interface group name.
INTERFACE INCLUDED	Indicates the included interfaces.
POLICY	Indicates a load balancing policy.
STATE	Indicates the state of an interface group.

4 APP-PROXY Commands

4.1 app-proxy enable

Use this command to enable APP-PROXY. Use the **no** form of this command to disable APP-PROXY.

app-proxy enable

no app-proxy enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults APP-PROXY is enabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to enable APP-PROXY.

Configuration Examples The following example enables APP-PROXY.

```
FS#config
FS(config)#app-proxy enable
```

Verification Run the **show app-proxy enable** command to check whether APP-PROXY is enabled.

4.2 app-proxy http enable

Use this command to enable HTTP APP-PROXY. Use the **no** form of this command to disable HTTP APP-PROXY.

app-proxy http enable

no app-proxy http enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults HTTP APP-PROXY is enabled by default.

Command Mode Global configuration mode

Default Level

14

Usage Guide

This command is used to enable HTTP APP-PROXY.

Configuration Examples

The following example enables HTTP APP-PROXY.

```
FS#config
FS(config)#app-proxy http enable
```

Verification

Run the **show app-proxy enable** command to check whether HTTP APP-PROXY is enabled.

4.3 show app-proxy enable

Use this command to display the status of APP-PROXY function switches.

show app-proxy enable

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

This command is used to display the status of APP-PROXY function switches.

Configuration Examples

The following example displays the status of APP-PROXY function switches.

```
FS#show app-proxy enable
app-proxy                              :     Y
app-proxy http                         :     Y
app-proxy udp                          :     Y
app-proxy url                          :     Y
app-proxy dns                          :     Y
```

Field description:

Field	Description
app-proxy	APP-PROXY general switch
app-proxy http	HTTP APP-PROXY switch
app-proxy udp	UDP traffic blocking switch
app-proxy url	DNS traffic diversion library enabling switch
app-proxy dns	APP-PROXY DNS function switch

5 User Session Limit Commands

5.1 flow-pre-mgr { down-deny | down-permit }

Use this 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-ange** { *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** } } } }

Use the **no** form of this command to disable the function.

no flow-pre-mgr { **down-deny** | **down-permit** } *id*

Parameter Description

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

Defaults N/A

Command Mode Global configuration mode

Default level

14

Usage Guide

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 uplink new packet filtering command when there is a large number of ACEs.

The source IP address cannot be set to **any** when the uplink new sessions filtering command is configured.

The destination IP address cannot be set to **any** when the downlink new sessions filtering command is configured.

The ID of rule Permit and Deny is different. Thus, conflicts will not occur.

The priority of rule Deny is higher than rule Permit.

Configuration Examples

#Only port 80 can be accessed by external devices. External IP 110.110.110.24 cannot ping the device with IP 172.18.124.118.

```
FS# configure terminal
FS(config)# flow-pre-mgr down-deny 1 icmp src-host 110.110.110.24 dst-host 172.18.124.118
FS(config)# flow-pre-mgr down-permit 1 tcp src-host any src-port any dst-host 172.18.124.118 dst-port 80
FS(config)# flow-pre-mgr down-permit 2 udp src-host any src-port any dst-host 172.18.124.118 dst-port 80
```

Verification

1. Use the **show flow-pre-mgr drop-count** command to check the packet loss status.
2. Use the **show ip session filter** command to check the number of packets matched per rule.

5.2 flow-pre-mgr { up-deny | up-permit }

Use this 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** } } } }

Use the **no** form of this command to disable the function.

no flow-pre-mgr { **up-deny** | **up-permit** } *id*

Parameter Description

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

Defaults

N/A

Command Mode

Global configuration mode

Default level

14

Usage Guide

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 the uplink new sessions filtering command is configured.

The destination IP address cannot be set to **any** when the downlink new sessions filtering command is configured.

The ID of rule Permit and Deny is different. Thus, conflicts will not occur.

The priority of rule Deny is higher than rule Permit.

Configuration Examples

#Block IP 192.168.1.24 from accessing the network. Allow other IPs in internal network segment 192.168.1.0/24 and 172.18.1.0/24 to access the network.

```
FS# configure terminal
FS(config)# flow-pre-mgr up-deny 1 ip src-host 192.168.1.24 dst-host any
FS(config)# flow-pre-mgr up-permit 1 ip src-subnet 192.168.1.0 255.255.255.0 dst-host any
FS(config)# flow-pre-mgr up-permit 2 ip src-subnet 172.18.1.0 255.255.255.0 dst-host any
```

Verification

1. Use the **show flow-pre-mgr drop-count** command to check the packet loss status.
2. Use the **show ip session filter** command to check the number of packets matched per rule.

5.3 flow-pre-mgr access-list

Use this command to configure the ACL-based session limit.

flow-pre-mgr *rule-id* **access-list** *acl-number* **action** { **block** | **by-pass** | { **trust total-limit** *total-limit-number* } }

Use the **no** form of the command to disable the function.

no flow-pre-mgr *rule-id*

Parameter Description

Parameter	Description
rule-id	Rule identifier ranging from 1 to 50. When the configured identifier was used, the configuration will fail with prompt of collision.
acl-number	Rule-associated ACL number, ranging from 1 to 199.
total-limit *total-limit-number*	Total limit number of streaming ACL sessions, whose range depends on the device RAM, where 0 represents that there is no limit.

Defaults

N/A

Command Mode

Global configuration mode

Default level

14

Usage Guide

5. You can use the following control mode of the ACL-based streaming session: block, by-pass or trust. To delete the relative configuration, you can use the **no** form of the **flow-pre-mgr id** command in global configuration mode.
6. Configured rules have their priorities. The latest configured rule is with the highest priority level.
7. You cannot configure any streaming session limit per IP address based on ACL.
8. 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.
9. 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 outside network IP address, and the destination interface with the outside network interface.
10. 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.
11. 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.
12. 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.
13. 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.

⚠ The ACL must be configured first.

Configuration Examples

#Configure an ACL entry for the stream between a matched device and the outside network IP address: 220.200.20.20, and set the total limit number of streaming sessions to 30.

```
FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)#ip access-list extended 120
FS(config-ext-nacl)#permit ip any host 220.220.20.20
FS(config-ext-nacl)#deny ip any any
FS(config-ext-nacl)#exit
FS(config)#flow-pre-mgr 2 access-list 120 action trust total-limit 30
```

#Create streaming sessions for the IP segment of the internal network only when the internal IP segment is 192.168.1.0/24, and treat the rest as by-pass.

```
FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)#ip access-list standard 2
FS(config-std-nacl)#deny 192.168.1.0 0.0.0.255
FS(config-std-nacl)#permit any
FS(config-ext-nacl)#exit
FS(config)# flow-pre-mgr 1 access-list 1 action by-pass
```

Verification

1. Use the **show flow-pre-mgr rule-info** command to display configured rules and the matching situation of sessions;
2. Use the **show flow-pre-mgr ip-info** command to display IP session and the limit.

Prompt Information

If the Rule ID was used, then error message is prompted.

```
Rule id already exists, please delete it first
```

Common Errors

Fail to configure specified ACL.

5.4 flow-pre-mgr enable

Use this command to enable the global session limit.

flow-pre-mgr enable

Use the **no** form of the command to disable the function.

no flow-pre-mgr enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Enabled by default.

Command Mode

Global configuration mode

Default level

14

Usage Guide

You can use this command to enable the global session limit, which is enabled by default. You can use the **no** form of the **no flow-pre-mgr enable** command to disable the function.

Configuration Examples

#Use the **no** form of the command to disable the function.

```
FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# no flow-pre-mgr enable
```

Verification

Use the **show running-config** command to display whether there is no flow-pre-mgr enable; if not, then the function is enabled.

5.5 flow-pre-mgr new-session-limit { specify | specify-range | specify-subnet }

Use this command to configure the new session limit for real IP addresses, where some special IP addresses (such as those of servers) requires a wide range of the session limit**.**

flow-pre-mgr new-session-limit { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number*

Use the **no** form of this command to disable the function.

no flow-pre-mgr new-session-limit { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* }

Parameter Description

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 10,000,000

Defaults

Default value is 0, that is, without limit

Command Mode

Global configuration mode

Default level

14

Usage Guide

You can configure the new session limit for real IP addresses, where some special IP addresses (such as those of servers) requires a wide range of the session limit**.**

Configuration Examples

#Set the new session limit of the internal real IP to less than 1,000 and that of the DNS sever 192.168.1.112 to 10,000.

```
FS# configure terminal
FS(config)# flow-pre-mgr new-session-limit real-host limit 1000
FS(config)# flow-pre-mgr new-session-limit specify-subnet 192.168.1.0 255.255.255.0 limit 10000
```

Verification

1. Use the **show flow-pre-mgr new-session-limit** command to display the configuration.
2. Use the **show flow-pre-mgr drop-count** command to check the packet loss status.
3. Use the **show flow-pre-mgr new-session-limit attack** command to check the attacks.

5.6 flow-pre-mgr new-session-limit { start-up | virtual-host | real-host }

Use this command to configure the new session limit of all virtual IP addresses within 3 minutes after start up; configure the new session limit of all virtual IP addresses after 3 minutes after start up; or configure the new session limit of real IP addresses and drop the flow platforms that surpass the limit.

flow-pre-mgr new-session-limit { **start-up** | **virtual-host | real-host** } **limit** *limit-number*

Use the **no** form of this command to disable the function.

no flow-pre-mgr new-session-limit { **start-up** | **virtual-host | real-host** }

Parameter Description

Parameter	Description

limit-number	New session limit.Range: 0 to 10,000,000

Defaults

Default value is 0, that is, without limit

Command Mode

Global configuration mode

Default level

14

Usage Guide

You can configure a new session limit for the internal IP address to prevent bulk new attacks on the device or outer network caused by virus of the internal real IP address.

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.

Configuration Examples

#Set the new session limit of all virtual IPs to 20,000 within 3 minutes after the start up; set the new session limit of virtual IP to 3000; and set the new session limit of real IP to 300.

```
FS# configure terminal
FS(config)# flow-pre-mgr new-session-limit start-up limit 20000
FS(config)# flow-pre-mgr new-session-limit virtual-host limit 3000
FS(config)# flow-pre-mgr new-session-limit real-host limit 300
```

Verification

1. Use the **show flow-pre-mgr new-session-limit** command to display the configuration.
2. Use the **show flow-pre-mgr drop-count** command to check the packet loss status.
3. Use the **show flow-pre-mgr new-session-limit attack** command to check the attacks.

5.7 flow-pre-mgr priority-swap

Use this command to swap the priority levels of two rules.

flow-pre-mgr priority-swap *rule-id1 rule-id2*

Parameter Description

Parameter	Description
rule-id1	Rule ID whose priority level to be swapped
rule-id2	Rule ID whose priority level to be swapped

Defaults

N/A

Command Mode

Global configuration mode

Default level

14

Usage Guide

You can use this command to swap the priority levels of two rules.

Configuration Examples

#Swap the priority levels of rule 1 and rule 2.

```
FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-pre-mgr priority-swmp 1 2
```

Verification

Use the **show flow-pre-mgr rule-info** command to display the swapped priority level of rules. The priority level of this command is arranged from high to low.

Common Errors

If rule-id 1 or rule-id 2 does not exist, this command will swap nothing.

5.8 flow-pre-mgr protocol-enable

Use this command to allow the OSPF, VRRP, and RIP protocols.

flow-pre-mgr protocol-enable

Use the **no** form of this command to block the OSPF, VRRP, and RIP protocols.

no flow-pre-mgr protocol-enable

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults

Allow the OSPF, VRRP, and RIP protocols by default.

Command Mode

Global configuration mode

Default level

14

Usage Guide

Order: ip session filter→ protocols allowing → IP new session rate limit →buffer protection

Configuration Examples

#Enable the function to allow the protocols.

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# flow-pre-mgr protocol-enable
```

Verification

Use the **show flow-pre-mgr protocol-enable** to check whether the protocols allowing function is enabled.

5.9 flow-pre-mgr subscriber

Use this command to configure the session limit based on subscriber/subscriber group.

flow-pre-mgr *rule-id* **subscriber** *subs_name* **action {block | by-pass | {trust total-limit** *total-limit-number* **per-ip-limit** *per-limit-number* **}}**

Use the **no** form of this command to disable the function.

no flow-pre-mgr *rule-id*

Parameter Description

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 ACL session based on subscriber/subscriber group, whose range depends on the device RAM, where 0 represents that there is no limit.
per-limit-number	Limit number of the streaming ACL session per IP address of subscriber/subscriber group, whose range depends on the device RAM but not larger than total-limit-number, where 0 represents that there is no limit.

Defaults

N/A

Command Mode

Global configuration mode

Default level

14

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 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.

⚠ You should first enable the layer23 classification and configure corresponding subscriber/subscriber group information

Configuration Examples

#Set subscriber group "UserGroup A" to allowing 5,000 streaming sessions created and 300 streaming sessions per IP address of "UserGroup A". New streaming session will be blocked after the limit is surpassed.

```
FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# subscriber static name UserGroupA parent /
FS(config)# subscriber static name UserA parent /UserGroupA ip-host 192.168.5.10
FS(config)# subscriber static name UserB parent /UserGroupA ip-host 192.168.5.11
FS(config)# flow-pre-mgr 1 subscriber UserGroupA action trust total-limit 5000 per-ip-limit 300
```

Verification

1. Use the **show flow-pre-mgr rule-info** command to display configured rules and the matching situation of sessions;
2. Use the **show flow-pre-mgr ip-info** command to display IP session and the limit.

Prompt Information

If the rule ID was obsessed, then error message is prompted.

```
Rule id already exists, please delete it first
```

Common Errors

Fail to enable the layer23 classification or configure corresponding subscriber/subscriber group information

5.10 flow-pre-mgr per-ip-limit udp-ratio

Use this command to configure the limit ratio of user/user group-based UDP sessions to total sessions.

flow-pre-mgr per-ip-limit udp-ratio *ratio*

Use the **no** form of this command to delete the limit ratio of user/user group-based UDP sessions to total sessions.

no flow-pre-mgr per-ip-limit udp-ratio

Parameter

Parameter	Description

Description

ratio	Indicates the ratio of the per-IP-based UDP sessions of a user/user group to total sessions. The value range is 0 and from 30 to 80, of which **0** indicates no limitation.

Defaults The default value is 0, indicating no limitation.

Command Mode Global configuration mode

Default Level 14

Usage Guide Configure the per-IP-based session limit rule with the user/user group-based session quantity control mode of trust, and then configure the ratio of UDP sessions to total sessions.

The default value is **0**, indicating that UDP sessions are not limited.

The per-IP-based session limit rule with the user/user group-based session quantity control mode of trust must be configured first.

Configuration Examples #Configure no limitation on the total number of sessions created by all users. Each IP address can create at most 3000 sessions. The ratio of per-IP-based UDP sessions to total sessions is set to 50. If the limit is exceeded, new UDP sessions will be blocked.

```
FS# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
FS(config)# flow-pre-mgr 1 subscriber UserGroupA action trust total-limit 0 per-ip-limit 3000
FS(config)# flow-pre-mgr per-ip-limit udp-ratio 50
```

Verification Run the **show flow-pre-mgr ip-info** command to show the number of UDP sessions created by each IP address and the limit ratio of UDP sessions.

Prompt Information N/A

Common Errors The per-IP-based session limit rule with the user/user group-based session control mode of trust is not configured.

5.11 flow-pre-mgr total-limit

Use this command to configure the total-limit-number of session.

flow-pre-mgr total-limit *limit-number*

Use the **no** form of this command to disable the function.

no flow-pre-mgr total-limit

Parameter Description

Parameter	Description
limit-number	Total limit number of the global streaming session, whose range depending on the device RAM, where 0 represents that there is no limit.

Defaults

N/A

Command Mode

Global configuration mode

Default level

14

Usage Guide

1. 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.
2. 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.

Configuration Examples

#Set the total-limit-number of global streaming session to 200,000. When the session number reaches the limit, new stream cannot be created and will be blocked.

```
FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-pre-mgr total-limit 200000
```

Verification

1. Use the **show flow-pre-mgr rule-info** command to display configured rules and the matching situation of sessions;
2. Use the **show flow-pre-mgr ip-info** command to display IP session and the limit.

5.12 flow-pre-mgr upload-pps-limit [virtual-host limit]

Use this command to configure the limit of uploading packet rate for real IPs.

flow-pre-mgr upload-pps-limit [**virtual-host limit**] *limit-number*

Use the **no** form of this command to disable the function.

no flow-pre-mgr upload-pps-limit [**virtual-host limit**]

Parameter Description

Parameter	Description
limit-number	Limit of uploading packet speed, ranging from 0 to 10,000,000.

Defaults

Default value is 0, that is without limit

Command Mode

Global configuration mode

Default level

14

Usage Guide

It is recommended to enable this function when it is needed to prevent the upload flow attack. The function takes effect on real/virtual IP only. Each real/virtual IP's uploading packet rate will be counted respectively.

Configuration Examples

#Set the limit of uploading packet rate per IP address to 2,000.

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# flow-pre-mgr upload-pps-limit 2000
```

Verification

1. Use the **show flow-pre-mgr upload-pps-limit** command to display the configuration.
2. Use the **show flow-pre-mgr drop-count** command to display the packet loss status.

5.13 flow-pre-mgr upload-pps-limit { specify | specify-range | specify-subnet }

Use this command to configure the limit of uploading packet rate for specified IP addresses.

flow-pre-mgr upload-pps-limit { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number*

Use the **no** form of this command to disable the function.

no flow-pre-mgr upload-pps-limit { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* }

Parameter Description

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 10,000,000.

Defaults

N/A

Command Mode

Global configuration mode

Default level

14

Usage Guide

Normally, by enabling defense against the upload flow attack, you can use this command to customize the settings of some special IP addresses (such as the internal network server).

Configuration Examples

#Set the uploading packet speed of internal network subscribers to not more than 3,000 per second and the subscriber with the IP address of 192.168.1.2 to not more than 10,000 packets per second.

```
FS# configure terminal
FS(config)# flow-pre-mgr upload-pps-limit 3000
FS(config)# flow-pre-mgr upload-pps-limit specify 192.168.1.2 limit 10000
```

Verification

1. Use the **show flow-pre-mgr upload-pps-limit** command to display the configuration.
2. Use the **show flow-pre-mgr drop-count** command to display the packet loss status.

5.14 ip session filter

Use this command to configure a session filter.

ip session filter *acl-id*

Use the **no** form of this command to delete the session filter.

no ip session

filter

Parameter	Description
acl-id	Indicates the ACL ID

N/A

Global configuration mode

14

Use this command to per

mit the matched IP packets.

#Configure a session filter to permit only IP packets in the 192.168.1.0 network segment.

```
FS# configure terminal
Enter configuration comman
```

```
ds, one per line. End with CNTL/Z.
FS(config)# ip access-list extended 190
FS(config-ext-nacl)# 10 permit ip 192.168.1.0 0.0.0.255 any
FS(config-ext-nacl)# exit
FS(config)# ip
```

session filter 190

Use the **show flow-pre-mgr drop-count** command to display the packets filtered by ACL.

5.15 Show flow-pre-mgr drop-count

Use this command to display the log of buffer protection.

show flow-pre-mgr drop-count

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide You can use this command to count the packet loss of each function respectively.

Configuration Examples

#Display the number of packet loss.

```
FS#show flow-pre-mgr drop-count
DROP-TYPE                  DROP-PKT
==================================
Filter-pkt             42892
Session-real            0
Session-specify        0
Session-virtual        970
Session-cpu              0
PPS-real                 0
PPS-specify              0
PPS-virtual             0
Buff-real               0
Buff-virtual          0
```

5.16 show flow-pre-mgr ip-info

Use this command to display the session number of IP addresses and their session limits.

show flow-pre-mgr ip-info [*ip-address*]

Parameter Description

Parameter	**Description**
ip-address	Displays the session of specified IP addresses and their session limits
default	If no ip-address parameter is specified, then all IP addresses are displayed by default.

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide You can use this command to display the session number of IP addresses and their session limits.

Configuration Examples #Display the session limit of IP addresses and their session limits.

```
FS#show flow-pre-mgr ip-info
IP-ADDRESS               flow-cnt        flow-limit      UDP-fcnt       UDP-flimit
==============================================================================
===================
192.168.10.1            203             500              150            150
192.168.10.2            103             500              50             150
192.168.10.3            20              0                10             0
192.168.10.4            15              0                8              0
```

FS# Filed Interpretation

Field	Description
IP-ADDRESS	IP address
flow-cnt	Number of current sessions
flow-limit	Session limit
UDP-fcnt	Number of UDP sessions
UDP-flimit	UDP session limit

5.17 show flow-pre-mgr new-session-limit

Use this command to display configured rules preventing new session attack.

show flow-pre-mgr new-session-limit

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide You can use this command to display the new session limit configuration of the current device.

Configuration Examples #Display the configuration.

```
FS# show flow-pre-mgr new-session-limit
flow-pre-mgr new-session-limit start-up limit 20000
flow-pre-mgr new-session-limit virtual-host limit 10000
flow-pre-mgr new-session-limit real-host limit 1000
flow-pre-mgr new-session-limit specify-host 192.168.1.110 limit 5000
flow-pre-mgr new-session-limit specify-host 192.168.1.112 limit 10000
```

5.18 show flow-pre-mgr new-session-limit attack

Use this command to display the log of the latest new session attack.

show flow-pre-mgr new-session-limit attack

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide You can use this command to display the latest attack on the current device by the new session.

Configuration Examples #Display the configuration.

```
FS# show flow-pre-mgr new-session-limit attack
HOST-TYPE           HOST-IP             TIME
==========================================================
real-host                172.18.8.156              2014-10-16 14:15:28
```

5.19 show flow-pre-mgr rule-info

Use this command to display configured rules.

show flow-pre-mgr rule-info

Parameter	Description

N/A	N/A

Privileged EXEC mode, Global configuration mode, interface mode

14

You can use this command to display configured rules and the matching situation of sessions.

#Display configured rules and the matching situation of sessions.

```
FS#show flow-pre-mgr rule-info flow-pre-mgr total-limit 200000 (active)flow-pre-mgr 1 subscriber UserGroupA action trust total-limit 5000 per-ip-limit 300 (446 flows) (inactive)flow-
```

```
pre-mgr 2 access-list 120 action block (0 flows)
```

Filed Interpretation

Field
activ
inact
flows

5.20 show flow-pre-mgr upload-pps-limit

Use this command to display configured rules preventing upload flow attack.

show flow-pre-mgr upload-pps-limit

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default level 14

Usage Guide

You can use this command to display the configuration of upload packet speed limit per IP address.

Configuration Examples

#Display the configuration.

```
FS# show flow-pre-mgr upload-pps-limit
flow-pre-mgr upload-pps-limit 3000
flow-pre-mgr upload-pps-limit specify 192.168.1.30 limit 5000
flow-pre-mgr upload-pps-limit specify 192.168.1.20 limit 10000
```

6 Flow Control Commands

6.1 auto-pir

Use this command to enable the PIR dynamic adjustment function of flow control channel tree.

auto-pir enable [**interval** *NUM* [**root-rate** *Percentage*]] [**exclude-pass**]

Use this command to disable the PIR dynamic adjustment function of flow control channel tree.

no auto-pir enable

Parameter Description

Parameter	Description
NUM	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	Threshold of PIR suppression or restoration: It refers to the root channel bandwidth utilization ratio. The processing logic is as follows: ● If the parameter is above the threshold, PIR suppression check is triggered according to the ascending order of channel priority. If a channel rate exceeds CIR, its PIR is suppressed. ● If the parameter is below the threshold by 10%, PIR restoration is triggered. It is restored according to the descending order of channel priority. ● There is no processing if the parameter is between the two values. The value is 90 by default when the parameter is not configured. The configuration range is from 1 to 99. Take the default value 90 as an example. When the value is less than 80%, PIR restoration is triggered; when the value is greater than 90%, PIR suppression check is triggered; there is no processing when the value is between 80% and 90%.
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.

Defaults EG product is enabled by default. NPE product is disabled by default.

Command Mode Channel tree configuration mode

Default Level 14

Usage Guide This function applies to the scenario where the flow control equipment 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.

Configuration Examples

#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** *Name* [**inbound | outbound**] **auto-pir** command to test whether auto-pir can take effect.

6.2 change-priority

Use this command to switch the priorities of two policy rules under the same flow control group:

change-priority rule1 *rule1-num* **rule2** *rule2-num* [**by-rule-number**]

Parameter Description

Parameter	Description
rule1-num	No. of the first policy rule switched, which is the priority No. by default
rule2-num	No. of the second policy rule switched, which is the priority No. by default
by-rule-number	Indicates that *rule1 -num* and *rule2 -num* are rule numbers if a value is entered, but not the default priority number.

Defaults

N/A

Command Mode

Flow control group configuration mode

Default Level

14

Usage Guide

The priority number of policy rule can be displayed through the Pri_num field in **show flow-control-policy rule** [**group** *name*].

Configuration Examples

#Switch the priorities of two policy rules with the priority No. 1 and priority No. 2 under the flow control group group1. Note that 1 and 2 are priority numbers:

```
FS(config)# config
FS(config)# flow-control group1
FS(config-flow-control)# change-priority rule1 1 rule2 2
```

Verification

Use the **show flow-control-policy rule** [**group** *name*] command to display the details of all the policy rules or the policy rules under a specific flow control group.

6.3 channel-default

Use this command to specify the default flow control channel.

channel-default *channel-name*

Use this command to restore the default configuration.

no channel-default

Parameter Description

Parameter	Description
channel-name	Name of the configured flow control channel

Defaults The parameter is the root channel by default.

Command Mode Channel tree configuration mode

Default Level 14

Usage Guide By configuring this command, all the flows for which flow control strategy matching has failed will enter the specified default channel.

Configuration Examples #Specify the "depart5" channel on the flow control tree in the downlink direction of flow control group "test" as the default channel.

```
FS(config)#flow-control test
FS(config-flow-control)#channel-tree inbound
FS(config-channel-tree)#channel-default depart5
```

Verification Use the **show flow-control {***NAME***}** command to display the configuration of the whole flow control group.

6.4 channel-group

Use this command to create a flow control channel.

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**] }

Use this command to delete a flow control channel.

no channel-group *name*

Use this command to delete a shared pool of flow control channels.

no channel-group *name* **pool** *pool_name*

Parameter Description

Parameter	Description
name	Name of the created channel
parent	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	Name of the parent channel of the created channel, which must be a created channel
cir *cir_num*	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. The bandwidth of the root node cannot be 0.
pir *pir_num*	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. The value of PIR is equal to the PIR of the parent node by default. If the parent node does not exist, the PIR value is equal to the CIR value.
pri *pri_num*	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	FIFO queue
per-net	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*	Network segment mask, in the input range from 1 to 32; 32 indicates the fair queue based on each IP address; the parameter is 32 by default if no value is entered.
per-user	Fair queue per account; the number of internal queues is not fixed, and the fair packet sending opportunity is realized based on each account; the parameter applies to the congested channel.
per-pir *ppir_num*	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*	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*	Name of the shared pool to which the configured flow control channel is added.
reverse	(Optional) Reverse Per-net. The speed is limited for the external network segment (IP address), and for the public network segment

	of the accessed branch (VPN scenario). The parameter is forward Per-net by default.

Defaults

The flow control channel is not configured by default.

Command Mode

Channel tree configuration mode

Default Level

14

Usage Guide

6. Only one root channel can exist for one flow control tree, and cir and pir of the root channel need to be configured as the equal value;
7. When the channel cir is configured, the sum of the configured cir and cir of all of its peer channels should be smaller than or equal to cir of the parent channel; when the channel pir is configured, the configured pir must be smaller than or equal to pir of the parent channel;
8. Channels with higher priority will be first scheduled, and the packet loss probability is lower in the case of congestion;
9. The per-net queue and per-user queue are fair queues, and the configuration makes sense and embodies its characteristics of fair packet sending only in the case of congestion;
10. The network segment flow beyond the limit of per-net queue will enter the default queue of per-net queue; this default queue is at the lowest packet sending priority, and the bandwidth of network segment within the limit will be first guaranteed; besides, none of per-pir, limit and session-limit supports nesting, e.g., the root channel limits session-limit to 1000 and the sub-channel of root channel limits session-limit of BT to 500; actually, it means that the non-BT flow limit session-limit is 1000, and the BT limit is 500;
11. Only the bottom two layers of flow control tree can be added to the shared pool, i.e., only the leaf channel and its parent channel can be added to the shared pool and the shared pool must be created already;
12. For adding to the shared pool of Per-IP type, the channel type must be Per-IP, namely, it is Per-net and per-mask is 32; moreover, the limit cannot be greater than the shared pool limit;
13. The number of shared pool member channels cannot exceed 8;
14. The channel of per-user type cannot be added to the shared pool.

Configuration Examples

#Create a channel named "root" on the flow control tree in the downlink direction of the flow control group "test":

```
FS(config)#flow-control test
FS(config-flow-control)#channel-tree inbound
FS(config-channel-tree)#channel-group root parent null cir 50000 pir 50000 pri 4 fifo
```

Platform Description

6.5 channel-tree

Use this command to create a flow control channel tree.

channel-tree { **inbound** | **outbound** }

Use this command to delete a flow control channel tree.

[**no**] **channel-tree** { **inbound | outbound** }

Parameter Description

Parameter	Description
inbound	Downlink
outbound	Uplink

Defaults The flow control tree is not configured by default.

Command Mode Flow-control mode

Default Level 14

Usage Guide A flow control group should contain the flow control tree in the downlink direction and the flow control tree in the uplink direction.

Configuration Examples #Create a flow control tree in the downlink direction and a flow control tree in the uplink direction respectively in the flow control group "test":

```
FS(config)#flow-control test
FS(config-flow-control)#channel-tree inbound
FS(config-channel-tree)#exit
FS(config-flow-control)#channel-tree outbound
FS(config-channel-tree)#exit
```

Verification Use **show flow-control** { *NAME* } to display the configuration of the whole flow control group.

6.6 clear flow-control

Use this command to configure the description of flow control group.

clear flow-control *name* **statistics**

Parameter Description

Parameter	Description
name	Flow control group name, with the maximum length of 32 characters

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Clear the statistical information value of flow control group data.

Configuration Examples #Clear the statistical information of flow control group "Gi0/1":

```
FS# clear flow-control Gi0/1 statistics
```

6.7 comment

Use this command to configure the description of flow control group.

comment *Comment_String*

Use this command to delete a configured description field.

[**no**] **comment** *Comment_String*

Parameter Description

Parameter	Description
Comment_String	A description string, with the maximum length of 127 characters; spaces are not allowed between characters.

Defaults The description field is not configured by default.

Command Mode **flow-control** configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples #Configure the description field in flow control group "Gi0/1":

```
FS(config)#flow-control Gi0/1
FS(config-flow-control)# comment Dianxin-10M
```

Verification Use the **show flow-control** { *NAME* } command to display the configuration of the whole flow control group.

6.8 flow-control

Use this command to configure a flow control group.

flow-control { **statistics | log on |** *name* [**update bandwith** *In_bandwith Out_bandwith* [**perpir-update**]] }

Use this command to delete a specific flow control group.

no flow-control *name*

Parameter Description

Parameter	Description
statistics	Packet data information statistic switch of the flow control forwarding plane (the statistic switch is enabled by default except the high performance equipment)

log	Flow control log switch
on	Log switch
name	Name of the flow control group
In_bandwith	Expected downlink bandwidth size after update, in the input range from 500 kbps to 10000000 kbps
Out_bandwith	Expected uplink bandwidth size after update, in the input range from 500 kbps to 10000000 kbps
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.

.

Defaults Only flow control template configuration exists in the system by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide

1. Configure this command to access the flow control group mode. The flow control policy rule and flow control channel can be further configured based on this flow control group. Note that the flow control group must be applied to the WAN port to make the policy rule and channel take effect.
2. The update keyword is used to update the bandwidth size of existing flow control group. Here, bandwidth update affects the configuration of all the shared pools and channel bandwidths, all of which will be adjusted proportionally.

Configuration Examples

#Configure flow control policy group group1.

```
FS#config
FS(config)#flow-control group1
```

#Configure flow control policy group group2.

```
FS#config
FS(config)# flow-control group2
```

#Delete flow control policy group group1.

```
FS#config
FS(config)#no flow-control group1
```

#Update the Gi0/0 bandwidth size to 20 Mbps.

```
FS#config
FS(config)#flow-control Gi0/0 update bandwith 20000 20000
```

Verification Use the **show flow-control** { *NAME* } command to display the configuration of the whole flow control group.

6.9 flow-policy

Use this command to apply the flow control group to the WAN port and make the flow control policy rule and flow control policy channel configured under this policy group take effect:

flow-policy *name*

Use this command to cancel the application of a specific flow control group on the interface:

no flow-policy

Parameter Description

Parameter	**Description**
name	Name of the flow control group

Defaults

No flow control group is applied on the WAN port in the system by default.

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

This command can only be configured on the WAN port and cannot be used on the non-WAN port.

Configuration Examples

#Apply the flow control policy group group1 to interface gi0/1:

```
FS#config
FS(config)#interface gi0/1
FS(config-if-GigabitEthernet 0/1)#flow-policy group1
```

#Cancel application of the flow control policy group group1 on the interface gi0/1:

```
FS#config
FS(config)#interface gi0/1
FS(config-if-GigabitEthernet 0/1)#no flow-policy
```

Verification

Use the **show run** command to check whether flow control is configured under the interface.

6.10 flow-rule

Use this command to 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:

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*]

Use this command to delete a policy.

no flow-rule *num*

Use this command to disable a policy.

flow-rule *num* **disable**

Use this command to cancel policy disabling.

no flow-rule *num* **disable**

Parameter Description

Parameter	Description
num	No. of flow control policy rule, in the input range from 1 to 8192.
vlan-group-name	Name of the vlan-group object associated with policy rule; "any" indicates matching any object.
subscriber-name	Name of the subscriber object associated with policy rule; "any" indicates matching any object.
auth-group-name	Name of the authentication object associated with policy rule; "any" indicates matching any authentication object.
network-group-name	Name of the network-group object associated with policy rule; "any" indicates matching any object.
app-group-name	Name of the app-group object associated with policy rule; "any" indicates matching any object.
time-rang-name	Name of the time-rang object associated with policy rule
in-channel-name	Name of the in-channel associated with policy rule
out-channel-name	Name of the out-channel associated with policy rule
string	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.

Defaults No policy rule is configured in the system by default.

Command Mode Flow control group configuration mode

Default Level 14

Usage Guide

3. The policy rule with different num values but the same keyword cannot be configured.
4. According to the policy rule matching principle, the one configured late will take effect first. To make a policy rule take effect, two parts of the policy, and all the associated objects and channel objects must be configured, and the flow control group where the policy rule is has been applied to the WAN port.
5. When the policy configuration **Action** is pass, **in-channel** or **out-channel** is not configured. Then, speed is

not limited in the corresponding **in** or **out** direction. When neither direction is configured, speed is not limited in the two directions.

6. Policy refinement judgment principle: Object priorities are compared first: vlan object > Intranet IP object > authentication object > external network IP object > application identification object. When the object priority is the same, the same objects are compared according to the fact that the subclass is finer than the parent class. For example, Ali Wangwang is an instant messaging software; when all the other objects are the same, it is finer to use the Ali Wangwang policy in comparison to the policy that the application object uses instant messaging software.

Configuration Examples

#Under the flow control group group1, configure to restrict the egress bandwidth of the Administrative Department of a company to 3 Mbps.

```
FS#config
FS(config)#flow-control group1
FS(config-flow-control)#flow-rule 1 vlan-group any subscriber Administrative Department network-group any app-group any time-rang any
FS(config-flow-control)#flow-rule 1 action pass out-channel Administrative Department egress bandwidth 3 Mbps
```

#Under the flow control group group2, configure to prevent Tom at the administrative department of a company from accessing Sina in working hours.

```
FS#config
FS(config)#flow-control group1
FS(config-flow-control)#flow-rule 1 vlan-group any subscriber Administrative Department Tom network-group sina app-group any time-rang work
FS(config-flow-control)#flow-rule 1 action drop
```

6.11 flow-template

Use this command to copy a new configuration by adopting an existing flow control group as a template. 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**]

Parameter Description

Parameter	Description
Src_name	Copied source flow control group, i.e., name of the flow control group used as a template
Dst_name	Name of the created flow control group, which cannot be the same as *Src_name*
In_bandwith	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	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.

Defaults

-

Command Mode

Global configuration mode

Default Level

14

Usage Guide

7. Bandwidth update affects the configuration of all the shared pools and channel bandwidths, all of which will be adjusted proportionally.
8. Configuration copy is used to generate new configuration according to the existing flow control group configuration template, where bandwidth update can be regarded as bandwidth update executed for the newly created flow control group.

Configuration Examples

#Generate a new flow control group BBB according to the flow control group AAA, and update the bandwidth to 15 Mbps.

```
FS#config
FS(config)# flow-template copy AAA BBB bandwith 15000 15000
```

6.12 share-pool

Use this command to create a shared pool.

share-pool *Name* **rate** *num1* [**type** { **normal** | **per-ip** [**limit** *num2***l** }]

Use this command to delete a shared pool.

no share-pool *Name*

Parameter Description

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

Default Level

14

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.

Configuration Examples

Create a normal type shared pool *test* with 1000kbps bandwidth under the inbound flow control tree of flow control group 1.

```
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** { *NAME* } command to check the configuration of the flow control group.

Platform Description

6.13 show flow control

Use this command to display the flow control group configuration information. The configuration of all the flow control groups is displayed if no flow control group is not specified:
show flow-control [*Name*]

Use this command to display the flow control channel configuration information:
show flow-control *Name* { **inbound | outbound** } [**channel-group** *channel-name* [**detail**]]

Use this command to display the shared pool configuration information

show flow-control *Name* { **inbound** | **outbound** } [**share-pool** [*pool-name*]]

Use this command to display the auto-pir status information:
show flow-control *Name* [**inbound** | **outbound**] **auto-pir**

Parameter Description

Parameter	Description
Name	Name of the flow control group
inbound	Flow control tree in the downlink direction
outbound	Flow control tree in the uplink direction
channel-name	Flow control channel configuration, which is used together with the detail keyword to display the FIFO, SFQ and Per-net queue running status information
pool-name	Related display of the shared pool; all the pools are displayed if the name is not entered; the specific pool is displayed if the name is entered.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

If the **channel-group** *channel-name* keyword is entered, only the configuration information of corresponding channel is displayed; otherwise, the configuration information of all channels configured on the entire flow control channel tree is displayed.

Configuration Examples

#Display the specified flow control group: the configuration information of Gi0/6.

```
FS#sh flow-control test
flow-control test
 comment tpl-ibar
 !
 channel-tree inbound
  auto-pir enable interval 1 root-rate 90
  !
  channel-group root parent null cir 130000 pir 130000 pri 4 per-net per-mask 32 per-cir 130 per-pir 2000 limit 1000
  channel-group key parent root cir 65000 pir 91000 pri 0 per-net per-mask 32 per-cir 65 per-pir 78000 limit 1000
  channel-group normal parent root cir 52000 pir 91000 pri 4 per-net per-mask 32 per-cir 52 per-pir 78000 limit 1000
  channel-group unkey parent root cir 13000 pir 52000 pri 7 per-net per-mask 32 per-cir 13 per-pir 3003 limit 1000
  channel-default normal
 !
 channel-tree outbound
   no auto-pir enable
   !
   channel-group root parent null cir 130000 pir 130000 pri 4 per-net per-mask 32 per-cir 130 per-pir 2000 limit 1000
   channel-group key parent root cir 65000 pir 78000 pri 0 per-net per-mask 32 per-cir 65 per-pir 4998 limit 1000
   channel-group normal parent root cir 52000 pir 78000 pri 4 per-net per-mask 32 per-cir 52 per-pir 3003 limit 1000
   channel-group unkey parent root cir 13000 pir 52000 pri 7 per-net per-mask 32 per-cir 13 per-pir 3003 limit 1000
   channel-default normal
  !
 flow-rule 1000 app-group Other_Group time-range any
 flow-rule 1000 action pass in-channel normal out-channel normal default comment Match_Normal_Group_of_NON_VPN
 flow-rule 999 app-group Key_Group time-range any
 flow-rule 999 action pass in-channel key out-channel key default comment Match_Key_Group_of_NON_VPN
 flow-rule 998 app-group Unkey_Group time-range any
 flow-rule 998 action pass in-channel unkey out-channel unkey default comment Match_Inhib_Group_of_NON_VPN
 flow-rule 992 subscriber VIP time-range any
 flow-rule 992 action pass in-channel key out-channel key comment Match_VIP_Group_of_NON_VPN
 flow-rule 991 network-group Out_Server time-range any
 flow-rule 991 action pass in-channel key out-channel key comment Match_Out_Server_of_NON_VPN
 flow-rule 900 app-group TC_AD_Key time-range any
 flow-rule 900 action pass in-channel key out-channel key comment Match_AD_Key_of_NON_VPN
 flow-rule 900 disable
```

#Display the configuration information of the specified channel in the downlink direction.

```
FS#sh flow-control test inbound channel-group root
Group-name                              CIR        PIR        Pri   Schedule
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool    R
-------------------------------- -------- -------- ---- -------- ----------------------------------------    -
root                                  130000     130000     4      per-net    32/130/2000/
1000/0                                  0
```

#Display the configuration information of all the downlink channels of the channel tree.

```
FS#sh flow-control test inbound
Group-name                              CIR          PIR          Pri    Schedule
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool    R
-------------------------------- -------- -------- ---- -------- ----------------------------------------    -
Root                                130000          130000      4       per-net    32/130/2000/1000/
0/                              0
Key                                 65000           91000       0       per-net    32/65/78000/1000/
0/                              0
Normal                              52000           91000       4       per-net    32/52/78000/1000/
0/                              0
Unkey                               13000           52000       7       per-net    32/13/3003/1000/
0/                               0
```

Field explanation:

Field	Description
Group-name	Channel name
CIR	Committed information rate
PIR	Peak information rate
Pri	Channel priority
Schedule	Channel queue type
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool	CIDR/CIR/PIR/Limit/Sess-limit/Share-pool

#Display the shared pool configuration information in the uplink direction:

```
FS#show flow-control test outbound share-pool
Global pool:        14                  Global red obj:    0
Tree pool:          3


Share-pool          Rate            Type            Limit           Child
-------------- ---------- ---------- ---------- ----------
tcp                    200            Normal          NA                  1
udp                     150             Normal          NA                  1
p1                     100             Normal          NA                  2
```

Field explanation:

Field	Description
Global pool	Number of shared pool
Global red obj	Shared pools that reach the upper Tx packets limit. It is the statistics of all nodes of normal and per-IP type

	shared pools.
Tree pool	Number of shared pools of corresponding channel-tree
Share-pool	Name of shared pool
Rate	Limited rate of shared pool
Type	Type of shared pool
Limit	Max number of users supported. Takes effect only in per-IP type shared pool.
Child	Number of member channels. Note that only the channel that adds to the shared pool will be counted. For example, if a parent channel which has three sub channels is added, the statistics value will be one.

#Display the specified shared pool information in the uplink direction:

```
FS#show flow-control test3 outbound share-pool p1
Pool:       p1
Rate:       100         Type:       Normal      Limit:      NA
State:      Green       Child:      2           Active:     NA
Kill flow: 0

Group-name   Cir      Pir      Pri  Type       Limit     Share-pool
----------- ------ ------- ---- -------- -------- ----------
p1-tcp       150      500      4    fifo       NA        p1
p1-udp       100      500      4    fifo       NA        p1
```

Field explanation:

Field	Description
Pool	Number of shared pool
Rate	Limited rate of shared pool
Type	Type of shared pool
Limit	Max number of users supported. Takes effect only in per-IP type shared pool.

State	Takes effect only in normal type shared pool. Red means the upper Tx packets limit has reached, while Green is not. In Per-IP type shared pool, it is N/A.
Child	Number of member channels. Note that only the channel that adds to the shared pool will be counted. For example, if a parent channel which has three sub channels is added, the statistics value will be one.
Limit	Max number of users supported. Takes effect only in per-IP type shared pool.
Active	Number of active users. Takes effect only in per-IP type shared pool.
Kill flow	Number of killed flows. Takes effect only in per-IP type shared pool.
Group-name	Name of shared pool member channel
Cir	Min Bandwidth of shared pool member channel
Pir	Max bandwidth of shared pool member channel
Type	Type of shared pool member channel
Pri	Priority of shared pool member channel
Limit	Max number of users supported by shared pool member channel. Takes effect only in per-IP type shared pool.
Share-pool	Name of channel added to shared pool Note: if a member channel in the specified shared pool is not a leaf channel, the sub channel of it will be displayed. If the sub channel has been added to other shared pools, then the shared pool name will be displayed replacing the Share-pool field. Otherwise, the Share-pool field will be N/A.

6.14 show flow-control-policy group

Use this command to display details of a flow control group.

show flow-control-policy group

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Display the details of all the flow control groups in the system, including the flow control group name, flow control group No., interface index value used by the flow control group, and the total number of policy rules configured under this flow control group.

Configuration Examples

#Display the details of all the flow control groups in the system:

```
FS#show flow-control-policy group
group_name                      group_id   apply_ifx      policy_entries
group1                          0             6                 14
group2                          1             0                 4
```

Field explanation:

Field	Description
group-name	Name of the flow control group
group-id	No. of the flow control group
apply_ifx	Interface index value applied to the flow control group: "0" indicates tha it is not applied to any interface.
policy_entries	Number of flow control policy rules configured under this flow control group

6.15 show flow-control-policy rule

Use this command to display details of a flow control policy rule.

show flow-control-policy rule [**group** *name*]

Parameter Description

Parameter	Description
name	Name of the flow control group

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

The use case displays the details of all the policy rules in the system or the policy rules under a flow control group, including the No. of each policy rule, priority No., related interface index value of policy rule, id of each object, number of flows matched with this policy rule at present, maximum of sessions of this policy rule, and validity of this policy rule.

Configuration Examples

#Display the details of all the flow control groups in the system:

```
FS#sh flow-control-policy rule

Some comment:

| prio      : priority of the rule | grp        : group the rule located | rule      : rule number in group      |
| ifx       : interface correspond | vlan_id    : vlan identify              | subs_id : subscriber identify        |
| auth_id : auth_group identify    | net_wk_id : network identify          | app_id    : application identify      |
| in        : in-channel identify      | out        : out-channel identify      | ses_now : session hold now
|
| ses       : config session             | stat       : disable or enable        | ef        : the effect of the rule |

prio   grp rule   ifx   vlan_id      subs_id      auth_id      net_wk_id   app_id        in      out      ses_now
ses     stat ef
73     5     1000   0      4294967295 4294967295 4294967295 4294967295 4294967288 5        5         0
0        up     0
74     5     999    0      4294967295 4294967295 4294967295 4294967295 4294967290 1        1         0
0        up     0
75     5     998    0      4294967295 4294967295 4294967295 4294967295 4294967289 6        6         0
0        up     0
76     5     997    0      4294967295 4294967295 4294967295 4294967295 4294967295 4        4         0
0        up     0
77     5     996    0      4294967295 4294967295 4294967295 4294967295 0               3        3         0
0        up     0
78     5     995    0      4294967295 4294967295 4294967295 4294967295 0               2        2         0
0        up     0
79     5     994    0      4294967295 20069752      4294967295 4294967295 4294967295 2        2         0
0        up     0
80     5     993    0      4294967295 4294967295 4294967295 19787672      4294967295 2        2         0
0        up     0
81     5     992    0      4294967295 20069752      4294967295 4294967295 4294967295 1        1         0
0        up     0
82     5     991    0      4294967295 4294967295 4294967295 19787672      4294967295 1        1         0
0        up     0
83     5     900    0      4294967295 4294967295 4294967295 4294967295 4144963584 1        1         0
0        down 0
84     6     1000   0      4294967295 4294967295 4294967295 4294967295 4294967288 5        5         0
0        up     0
85     6     999    0      4294967295 4294967295 4294967295 4294967295 4294967290 1        1         0
0        up     0
86     6     998    0      4294967295 4294967295 4294967295 4294967295 4294967289 6        6         0
0        up     0
87     6     997    0      4294967295 4294967295 4294967295 4294967295 4294967295 4        4         0
0        up     0
88     6     996    0      4294967295 4294967295 4294967295 4294967295 0               3        3         0
```

```
0      up    0
89    6    995    0      4294967295 4294967295 4294967295 4294967295 0              2        2        0
0      up    0
90    6    994    0      4294967295 20069752     4294967295 4294967295 4294967295 2        2        0
0      up    0
91    6    993    0      4294967295 4294967295 4294967295 19787672     4294967295 2        2        0
0      up    0
92    6    992    0      4294967295 20069752     4294967295 4294967295 4294967295 1        1        0
0      up    0
93    6    991    0      4294967295 4294967295 4294967295 19787672     4294967295 1        1        0
0      up    0
```

Field explanation:

Field	Description
prio	Priority No. of the flow policy rule
grp	No. of the flow control group, indicating the flow control group to which this policy belongs
rule	Flow control policy No.
ifx	Interface index value belonging to the flow control policy rule: "0" indicates that the flow control group where this rule is has not been applied to the interface.
vlan_id	ID of the vlan-group object associated with the flow control policy rule: "0" indicates that this vlan-group object is not configured.
subs_id:	ID of the subscriber object associated with the flow control policy rule: "0" indicates that this subscriber object is not configured.
auth_id	ID of the auth-group object associated with the flow control policy rule: "0" indicates that this auth-group object is not configured.
net_wk_id	ID of the network-group object associated with the flow control policy rule: "0" indicates this network-group object.
app_id	ID of the app-group object associated with the flow control policy rule: "0" indicates this app-group object.
in	ID of the in-channel channel object associated with the flow policy rule; if the ID value is 0, this channel object is not configured; if the ID value is NA, this rule is not associated with the in-channel channel object.
out	ID of the out-channel channel object associated with the flow policy rule; if the ID value is 0, this channel object is not configured; if the ID value is NA, this rule is not associated with the out-channel channel object.
ses_now	Number of flows matched with this policy rule at present
ses	Maximum number of sessions of flow that can be matched according to the flow control policy rule
stat	"Down" indicates that this policy is disabled; "Up" indicates that this policy is not disabled.
ef	Effectiveness of the flow control policy rule; "0" indicates that the rule does not take effect; "1" indicates that the rule has taken effect.

6.16 small-packet

Use this command to forward the smaller packet through the specified channel first.

small-packet *name* [tcp | udp]

Parameter Description

Parameter	Description
name	Indicates name of the flow channel
TCP	Indicates that only small TCP packet is supported.
UDP	Indicates that only small UDP packet is supported.

Command Mode Channel tree configuration mode

Default Level 14

Usage Guide When the external bandwidth is little, it is recommended to enable the function on the uplink flow control channel to forward the smaller TCP packets through the key channel first. Thus, improve the flow throughput rate of small packets.

7 Flow Audit Commands

7.1 flow-audit data-store

Use this command to configure the storage period of table data (except the daily/weekly/monthly reports).

flow-audit data-store *num*

Use the **no** form of this command to delete the configuration.

no flow-audit data-store

Parameter Description

Parameter	Description
num	Indicates storage period in days. The value range is from 10 to 90.

Defaults

Table data is stored for 60 days by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the storage period of table data (except the daily/weekly/monthly reports).

Configuration Example

#Set the storage period of table data to 80 days.

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit data-store 80
```

Verification

Run the **show run** command to display the storage period of table data (except the daily/weekly/monthly reports).

7.2 flow-audit data-store day-report

Use this command to configure the storage period of historical data of daily reports.

flow-audit data-store day-report *num*

Use the **no** form of this command to delete the configuration.

no flow-audit data-store day-report

Parameter Description

Parameter	Description
num	Indicates the storage period in days. The value range is from 10 to 90.

Defaults

The historical data of daily reports is stored for 60 days by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the storage period of historical data of daily reports.

Configuration Example

#Set the storage period of daily reports to 30 days to save disk space.

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit data-store day-report 30
```

Verification

Run the **show run** command to display the storage period of historical data of daily reports.

7.3 flow-audit data-store month-report

Use this command to configure the storage period of historical data of monthly reports.

flow-audit data-store month-report *num*

Use the **no** form of this command to delete the configuration.

no flow-audit data-store month-report

Parameter Description

Parameter	Description
num	Indicates the storage period in months. The value range is from 1 to 12.

Defaults

The historical data of monthly reports is stored for 12 months by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the storage period of historical data of monthly reports.

Configuration Example

#Set the storage period of monthly reports to six months.

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit data-store month-report 6
```

Verification

Run the **show run** command to display the storage period of historical data of monthly reports.

7.4 flow-audit data-store week-report

Use this command to configure the storage period of historical data of weekly reports.

flow-audit data-store week-report *num*

Use the **no** form of this command to delete the configuration.

no flow-audit data-store week-report

Parameter Description

Parameter	Description
num	Indicates the storage period in weeks. The value range is from 1 to 52.

Defaults

The historical data of weekly reports is stored for 8 weeks by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the storage period of historical data of weekly reports.

Configuration Example

#Set the storage period of weekly reports to 28 weeks to learn about the traffic trend of the gateway and save disk space.

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit data-store week-report 28
```

Verification

Run the **show run** command to display the storage period of historical data of weekly reports.

7.5 flow-audit enable

Use this command to enable flow monitoring and audit.

flow-audit enable

Use the **no** form of this command to disable flow monitoring and audit.

no flow-audit enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable flow monitoring and audit.

Configuration Example

#Enable flow monitoring and audit.

```
FS#config
FS(config)# flow-audit enable
```

#Disable flow monitoring and audit.

```
FS#config
FS(config)#no flow-audit enable
```

Verification Run the **show run** command to display the status of flow monitoring and audit.

7.6 flow-audit generate-report

Use this command to configure generation time of daily/weekly/monthly reports.

flow-audit generate-report *hour*

Use the **no** form of this command to delete the configuration.

no flow-audit generate-report

Parameter Description

Parameter	Description
hour	Indicates the storage period in hours. The value range is from 0 to 23.

Defaults Reports are generated at 03:00 by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure generation time of daily/weekly/monthly reports.

Configuration Example #Set the generation time of daily/weekly/monthly reports to 05:00 if the services are busy at 03:00.

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit generate-report 5
```

Verification Run the **show run** command to display generation time of daily/weekly/monthly reports.

7.7 flow-audit hard-disk-quota

Use this command to configure the hard disk space quota available for flow monitoring.

flow-audit hard-disk-quota *percent*

Use the **no** form of this command to delete the configuration.

no flow-audit generate-report

Parameter Description

Parameter	Description
percent	Indicates a percentage. The value range is from 1 to 100.

Defaults The hard disk space quota available for flow monitoring is 50% of the total capacity by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure the hard disk space quota available for flow monitoring.

Configuration #Set the hard disk space quota available for flow monitoring to 30% to save disk space.

Example

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit hard-disk-quota 30
```

Verification Run the **show run** command to display the hard disk space quota available for flow monitoring.

7.8 flow-audit rt-refresh

Use this command to configure the update frequency of real-time traffic information.

flow-audit rt-refresh *num*

Use the **no** form of this command to restore the default configuration.

no flow-audit rt-refresh

Parameter Description

Parameter	Description
num	Indicates the update frequency. The default update frequency is 30 seconds.

Defaults Flow is refreshed at a frequency of 30 seconds by default.

Command Mode Global configuration mode

Usage Guide Use this command to change the update frequency of real-time traffic information.

Configuration Example #Set the update frequency of real-time traffic information to the default value. To display the traffic information in a more real-time manner, set the update frequency to 10 seconds.

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit rt-refresh 10
```

Verification Run the **show run** command to display the configuration result.

7.9 flow-audit vpn

Use this command to configure the flow monitoring mode of VPN.

flow-audit vpn { **inside-ip** | **outside-ip** }

Parameter Description

Parameter	Description
N/A	N/A

Defaults Flow monitoring of VPN is based on extranet IP addresses by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to change the flow monitoring mode of VPN according to actual needs.

Configuration Example

#Configure the headquarters as a VPN server and check traffic of different branches (through VPN dialup).

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit vpn outside-ip
```

#Configure branches as VPN clients, and change flow monitoring to be based on intranet IP addresses to check VPN access of each employee.

```
FS#config
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# flow-audit vpn inside-ip
```

Verification

Run the **show run** command to display the flow monitoring mode of VPN.

7.10 show flowrate

Use this command to display traffic information of the global system or on a specified interface at the present time, in the past few hours, or in a specified time period.

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**]]

Parameter Description

Parameter	**Description**
interface-name	Indicates the name of an interface.
hour	Indicates the number of the latest hours.
begin-year	Indicates the start year of a period.
begin-month	Indicates the start month of a period.
begin-day	Indicates the start day of a period.
begin-hour	Indicates the start hour of a period.
begin-minute	Indicates the start minute of a period.
end-year	Indicates the end year of a period.
end-month	Indicates the end month of a period.
end-day	Indicates the end day of a period.
end-hour	Indicates the end hour of a period.

end-minute	Indicates the end minute of a period.
begin-hour2	Indicates the start hour 2 of a period.
end-hour2	Indicates the end hour 2 of a period.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display real-time traffic information of the global system or a specified interface.

- Specify the keyword **global** to display real-time traffic information of the global system, and specify the keyword **interface** to display real-time traffic information of the interface.
  Examples:
  show flowrate global (displaying real-time traffic information of the global system)
  show flowrate interface gi0/3 (displaying real-time traffic information on the interface Gi0/3)

Configuration Example #Display current traffic information on the interface GE0/1.

```
FS# show flowrate interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
Pass input rate: 979685 bits/sec, 114 packets/sec
Pass output rate: 107233 bits/sec, 60 packets/sec
Drop input rate: 130 bits/sec, 5 packets/sec
Drop output rate: 210 bits/sec, 4packets/sec
```

#Display real-time traffic information of the global system.

```
FS# show flowrate global
global
Pass Input rate:          184592 bits/sec,          33 packets/sec
Pass Output rate:          30940 bits/sec,          28 packets/sec
Drop Input rate:               0 bits/sec,           0 packets/sec
Drop Output rate:              0 bits/sec,           0 packets/sec
```

7.11 show flowrate application

Use this command to display traffic information of applications, application groups, or application classes of the global system or a specified interface at the present time or in a specified time period.

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**]

Parameter Description

Parameter	Description
interface-name	Indicates the name of an L3 interface, which is used in gateway mode.
subscriber-name	Indicates a username.
subscriber-group	Indicates the name of a user group.
auth-group	Indicates the name of an authenticated object group.
auth-name	Indicates the name of an authenticated object.
Ip-address	Specifies an IP address.
application-group	Indicates the name of an application group.
application-type	Indicates an application class.
application-name	Indicates the name of an application.
hour	Indicates the number of the latest hours.
begin-year	Indicates the start year of a period.
begin-month	Indicates the start month of a period.
begin-day	Indicates the start day of a period.
begin-hour	Indicates the start hour of a period.
begin-minute	Indicates the start minute of a period.
end-year	Indicates the end year of a period.
end-month	Indicates the end month of a period.
end-day	Indicates the end day of a period.
end-hour	Indicates the end hour of a period.
end-minute	Indicates the end minute of a period.
begin-hour1	Indicates the start hour 1 of a period.
end-hour1	Indicates the end hour 1 of a period.
begin-hour2	Indicates the start hour 2 of a period.
end-hour2	Indicates the end hour 2 of a period.
n	Specifies the first n records.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display real-time traffic information of related applications.

- Specify the keyword **global** to display real-time traffic information of applications, application groups, or application classes of the global system, specify the keyword **interface** to display such information of a specified interface, and specify the keyword **VWAN** to display such information of acceleration channels. If no keyword is entered, real-time traffic information of applications is displayed. If the keyword **by-group** is used, real-time traffic information of application groups is displayed. If the keyword **by-type** is used, real-time traffic information of application classes is displayed.

Examples:

show flowrate application global (displaying real-time traffic information of applications in the global system)

show flowrate application interface gi0/3 (displaying real-time traffic information of different applications on the interface Gi0/3)

show flowrate application interface gi0/3 by-group (displaying real-time traffic information of all application groups on the interface Gi0/3)

show flowrate application interface gi0/3 by-type (displaying real-time traffic information of all application classes on the interface Gi0/3)

show flowr app vwan (displaying real-time traffic information of applications of acceleration channels)

- Specify the keyword **top** and parameter **n** to display the first n records of the ranking result.

  Example:

  show flowrate application interface gi0/3 order by pass download desc top 5 (querying real-time traffic information of applications on the interface Gi0/3, and displaying the first five records in descending order of download traffic)

- Specify one or more keywords (**subscriber**, **subscriber-group**, **auth-subs-group**, **auth-subs**, **ip**) to display real-time traffic information of applications.

  Example:

  show flowrate application interface gi0/3 ip 192.168.1.5 (displaying real-time traffic information of the application with the IP address 192.168.1.5 on the interface Gi0/3)

  This command supports statistics collection by group or type, display of user traffic information by user or user group, and ranking of traffic information in ascending or descending order based on application names and passed or discarded uplink/downlink traffic.

Configuration Example

#Display current application traffic on the interface GE0/1 in gateway mode.

```
FS# show flowrate application interface gigabitEthernet 0/1
path:GigabitEthernet 0/1
count: 1
Application        Application-group      Application-type
PASS:      Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
DROP:       Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
App1                       instant messaging                     Other application group
62597                      65955                           15                          17
0                           0                              0                           0
```

#Display application traffic information of the global system.

```
FS# show flowr app global
global
```

```
count: 4
Application                Application-group       Application-type
PASS:      Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
DROP:      Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
Tencent resource                   P2P              Unkey_Group
211                    249                    0                       0
0                      0                      0                       0
QQ-login|chat               instant messaging              Key_Group
286                    373                    0                       0
0                      0                      0                       0
IP application                   IP group                  Other_Group
20014                  70481                  12                      12
0                      0                      0                       0
telnet                      remote access protocol              Other_Group
64                     153                    0                       0
0                      0                      0                       0
```

#Display real-time application traffic information of acceleration channels.

```
FS# show flowr app vwan
vwan
count: 3
Application                Application-group       Application-type
PASS:      Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
DROP:      Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
Tencent resource                   P2P              Unkey_Group
786                    565                    0                       0
0                      0                      0                       0
QQ-login|chat               instant messaging              Key_Group
211                    373                    0                       0
0                      0                      0                       0
IP application                   IP group                  Other_Group
20014                  70481                  12                      12
0                      0                      0                       0
```

7.12 show flowrate ip

Use this command to display traffic information of the global system or on a specified interface at the present time, in the past few hours, or in a specified time period.

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** }]

Parameter Description

Parameter	Description
interface-name	Indicates the name of an interface, which is used in gateway mode.
subscriber-group	Indicates the name of a user group.
subscriber-name	Indicates a username.
auth-group	Indicates the name of an authenticated object group.
auth-name	Indicates the name of an authenticated object.
Ip-address	Specifies an IP address.
application-name	Indicates the name of an application.
application-group	Indicates the name of an application group.
application-type	Indicates an application class.
hour	Indicates the number of the latest hours.
begin-year	Indicates the start year of a period.
begin-month	Indicates the start month of a period.
begin-day	Indicates the start day of a period.
begin-hour	Indicates the start hour of a period.
begin-minute	Indicates the start minute of a period.
end-year	Indicates the end year of a period.
end-month	Indicates the end month of a period.
end-day	Indicates the end day of a period.
end-hour	Indicates the end hour of a period.
end-minute	Indicates the end minute of a period.
begin-hour1	Indicates the start hour 1 of a period.
end-hour1	Indicates the end hour 1 of a period.
begin-hour2	Indicates the start hour 2 of a period.
end-hour2	Indicates the end hour 2 of a period.
n	Specifies the first n records.

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display real-time traffic information of related users.

- Specify the keyword **global** to display real-time traffic information of users of the global system, specify the keyword **interface** to display such information of a specified interface, and specify the keyword **VWAN** to display such information of acceleration channels.

  Examples:

  show flowrate ip global (displaying real-time traffic information of users of the global system)

  show flowrate ip interface gi0/3 (displaying real-time traffic information of users on the interface Gi0/3)

  show flowr ip vwan (displaying real-time traffic information of users of acceleration channels)

- Specify the keyword **top** and parameter **n** to display the first n records of the ranking result.

  Example:

  show flowrate ip interface gi0/3 order by pass download desc top 5 (querying real-time traffic information of users on the interface Gi0/3, and displaying the first five records in descending order of download traffic)

- Specify one or more keywords (**application**, **application-group**, and **application-type**) to display real-time traffic information of applications.

  Example:

  show flowrate ip interface gi0/3 application PPTP (displaying real-time traffic information of the application PPTP on the interface Gi0/3)

  This command supports statistics collection of traffic information by group.

Configuration Example

#Display current traffic information of users on the interface GE0/1 in gateway mode.

```
FS# show flowrate ip interface gigabitEthernet 0/1

Subscriber                    ip

PASS: Upload(bps)     Download(bps)    Upload(pps)      Download(pps)

DROP: Upload(bps)     Download(bps)    Upload(pps)      Download(pps)

/User_groupA/User_nameA 2.2.2.92

230                   134              0                0

0                     0                0                0

/User_groupB/User_nameB    172.18.3.67

259                   153              0                0

0                     0                0                0
```

#Display real-time traffic information of users of the global system.

```
FS# show flowr ip global

global

subscriber              ip
```

```
PASS: Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
DROP: Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
/172.18.3.24            172.18.3.24
896                     1008                   1                     1
0                       0                      0                     0
/172.18.3.110           172.18.3.110
7526                    63712                  9                     9259
0                       0                      0                     0
/192.168.183.118            192.168.183.118
18116                   68729                  10                    10
0                       0                      0                     0
```

7.13 show flowrate ip-application

Use this command to display real-time traffic information of IP addresses or applications of the global system or a specified interface.

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*]]

Parameter Description

Parameter	Description
interface-name	Indicates the name of an interface, which is used in gateway mode.
subscriber-group	Indicates the name of a user group.
subscriber-name	Indicates a username.
auth-group-name	Indicates the name of an authenticated object group.
auth-name	Indicates the name of an authenticated object.
ip-address	Specifies an IP address.
application-name	Indicates the name of an application.
application-group	Indicates the name of an application group.
application-type	Indicates an application class.
n	Specifies the first n records.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display real-time traffic information of related IP addresses or applications.

- Specify the keyword **global** to display the real-time traffic information of IP addresses or applications of the global system, and specify the keyword **interface** to display such traffic information of a specified interface.
  Examples:
  show flowrate ip-application global ip 192.168.1.3 (displaying traffic information of the IP addresses or applications of the global system
  show flowrate ip-application interface gi0/3 ip 192.168.1.3 (displaying traffic information of the application with the IP address 192.168.1.3 on the interface Gi0/3)
- Specify the keyword **top** and parameter **n** to display the first n records of the ranking result.
  Example:
  show flowrate ip-application interface gi0/3 ip 192.168.1.3 order by pass download desc top 5 (querying current traffic information of the applications with the IP address 192.168.1.3 on the interface Gi0/3, and displaying the first five records in descending order of download traffic)

Configuration Example

#Display traffic information of the application with the IP address 172.18.36.102 on the interface GE0/1 in gateway mode.

```
FS# show flowrate ip-application interface gigabitEthernet 0/1
ip 172.18.36.102
path:GigabitEthernet 0/1
Subscriber    ip      Application    Application-group    Application-type
PASS: Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
DROP: Upload(bps)       Download(bps)     Upload(pps)       Download(pps)
/user_groupA/user_nameA    172.18.36.102     applicationA     application_groupA       key application group
46003                   2093107                 93                        173
0                       0                       0                         0
/user_groupA/user_nameB 172.18.36.102     applicationB    application_groupB      key application group
46001                   2093102                 193                        173
0                       0                       0                         0
/user_groupA/user_nameC172.18.36.102     applicationC application_groupC    key application group
4003                   1093107                 63                         73
0                       0                       0                         0
```

7.14 show online ip

Use this command to display Internet access duration and traffic information of the online IP addresses of the global system or a specified interface at the present time or in a specified time period.

show online ip {**global** | **interface** *interface-name*} [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] [**vip**] | [**auth** *auth-name*] [**auth-group** *auth-group*]] [**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-interval** *begin-hour* **to** *end-hour* [*begin-hour2* **to**

end-hour2]]}] [**order-by** {{**pass** | **drop**} {**upload** | **download**} | **ip** | **subscriber-group** | **subscriber** | **auth-group** | **auth** } {**desc** | **asc**}[**top** n]]

Parameter Description

Parameter	Description
interface-name	Indicates the name of an L3 interface, which is used in gateway mode.
subscriber-name	Indicates a username.
subscriber-group	Indicates the name of a user group.
auth-name	Indicates the name of an authenticated object.
auth-group	Indicates the name of an authenticated object group.
Ip-address	Specifies an IP address.
begin-minute	Indicates the start minute of a period.
end-minute	Indicates the end minute of a period.
begin-day	Indicates the start day of a period.
begin-month	Indicates the start month of a period.
begin-year	Indicates the start year of a period.
end-day	Indicates the end day of a period.
end-month	Indicates the end month of a period.
end-year	Indicates the end year of a period.
begin-hour	Indicates the start hour of a period.
end-hour	Indicates the end hour of a period.
begin-hour2	Indicates the start hour 2 of a period.
end-hour2	Indicates the end hour 2 of a period.
n	Specifies the first n records.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display Internet access duration and traffic information of online IP addresses.

- Specify the keyword **global** to display real-time traffic information of online IP addresses of the global system.
  Example:
  show online ip global (displaying current traffic information of online IP addresses of the global system)
- Specify the keyword **top** and parameter **n** to display the first n records of the ranking result.
  Example:
  show online ip global order by pass download desc top 5 (querying current traffic information of the online IP addresses of the global system, and displaying the first five records in descending order of download traffic)

Configuration Example #Display the first five records of Internet access duration and traffic information of the online IP addresses of the global system in decrement order according to the download traffic.

```
FS# show online ip global order-by pass download desc top 5
global
Subscriber
IP                       AuthType        LoginTime              OnlineTime(min)
PASS-Upload(KB)    PASS-Download(KB)    DROP-Upload(KB)       DROP-Download(KB)
/200.200.0.6
200.200.0.6                                  2013-7-3 15:38 1345
1405491                 655083                  0                         0
/200.200.0.7
200.200.0.7                                  2013-7-3 15:38 1345
1405489                 655044                  0                         0
/200.200.0.8
200.200.0.8                                  2013-7-3 15:38 1345
1405128                 655016                  0                         0
/200.200.0.2
200.200.0.2                                  2013-7-3 15:38 1345
1405221                 654959                  0                         0
/200.200.0.9
200.200.0.9                                  2013-7-3 15:38 1345
1404516                 654826                  0                         0
```

7.15 show online ip-application

Use this command to display the Internet access duration and traffic information of online IP addresses and applications of the global system or a specified interface at the present time.

show online ip-application {**global** | **interface** *interface-name*} [[**subscriber** *subscriber-name*] [**subscriber-group** *subscriber-group*] [**vip**] | [**auth** *auth-name*] [**auth-group** *auth-group*]] [**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-group** | **application**} {**desc** | **asc**}] [**offset** *start –record* {**limit** record-num}]

Parameter Description

Parameter	Description
interface-name	Indicates the name of an L3 interface, which is used in gateway mode.
subscriber-name	Indicates a username.
subscriber-group	Indicates the name of a user group.
auth-name	Indicates the name of an authenticated object.
auth-group	Indicates the name of an authenticated object group.

Ip-address	Specifies an IP address.
application-name	Indicates the name of an application.
application-group	Indicates the name of an application group.
application-type	Indicates an application class.
start-record	Indicates the start line of records.
record-num	Indicates the number of record lines.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Specify the keyword **global** to display the Internet access duration and traffic information of online IP addresses and applications of the global system at the present time. Specify the keywords (**ip**, **subscriber**, **subscriber-group**, **application**, and **application-group**) to display required information, specify the keyword **order-by** to decide the ranking sequence of the query results, and specify the keyword **top n** to display the first n records.

Configuration Example #Display the Internet access duration and traffic information of the applications with the IP address 172.18.181.63 of the global system.

```
FS# show online ip-application global ip 200.200.0.2
global
count:2
Subscriber
IP                    Application     Application-group    Application-type
LoginTime             OnlineTime(min)
PASS-Upload(KB)     PASS-Download(KB)     DROP-Upload(KB)        DROP-Download(KB)
/172.18.181.63
 172.18.181.63             BQQ    instant messaging    Other_Group
 2013-8-26 9:36              10456
   16703                 28711                  0                      0
/172.18.181.63
 172.18.181.63             MAPI    email protocol    Other_Group
 2013-8-26 9:36              10456
   5107                  8231                   0                      0
```

7.16 show online statistic

Use this command to display the numbers of IP addresses and sessions that are online at the present time, in the past few hours, or in a specified time period of the global system or a specified interface.

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*]]}]

Parameter Description

Parameter	Description
interface-name	Indicates the name of an L3 interface, which is used in gateway mode.
start-record	Indicates the start line of records.
record-num	Indicates the number of record lines.
hour	Indicates the number of the latest hours.
begin-year	Indicates the start year of a period.
begin-month	Indicates the start month of a period.
begin-day	Indicates the start day of a period.
begin-hour	Indicates the start hour of a period.
begin-minute	Indicates the start minute of a period.
end-year	Indicates the end year of a period.
end-month	Indicates the end month of a period.
end-day	Indicates the end day of a period.
end-hour	Indicates the end hour of a period.
end-minute	Indicates the end minute of a period.
begin-hour	Indicates the start hour of a period.
end-hour	Indicates the end hour of a period.
begin-hour2	Indicates the start hour 2 of a period.
end-hour2	Indicates the end hour 2 of a period.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the number of online IP addresses.

Specify the keyword **global** to display the number of online IP addresses of the global system.

Example:

show online statistics global (displaying the number of currently online IP addresses)

Configuration Example

#Display the number of currently online IP addresses of the global system.

```
FS# show online statistics global
global
online ip count: 500
```

8 Content Audit Commands

8.1 app-audit

Use this command to enable the application control audit optimization and set the time period in which the repeated application blocking of one IP address is not audited.
app-audit optimize-cache [*time*]

Use the **no** form of this command to disable the application control audit optimization.
no app-audit optimize-cache

Use this command to enable the application control audit optimization blocking.
app-audit optimize-deny

Use the **no** form of this command to disable the application control audit optimization blocking.
no app-audit optimize-deny

Parameter Description

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.

Defaults This function is enabled by default.

Command Mode Global configuration mode

Default Level 14

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.

Configuration Examples 1. The following example sets 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
```

2. The following example disables 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.

8.2 app-rule

Use this command to delete all application control audit rules in a policy group.

app-rule delete-all

Use this command to swap priorities of the application control audit access control rules.

app-rule priority-swap *rule-id1 rule-id2*

Use this command to add an application control audit rule to a content audit policy group.

app-rule *rule-id* **time-range** *time-name* **app-group** *app-group-name* **action** { **permit** | **deny** } [**audit**] [**vpn**] [**vip**] [**comment** *comment-string*]

Use the **no** form of this command to delete an application control audit rule.

no app-rule *rule-id*

Parameter Description

Parameter	Description
rule-id1	The ID of rule 1 of which the priority is to be swapped.
rule-id2	The ID of rule 2 of which the priority is to be swapped.
rule-id	The ID of a rule. A value range is 1 to 200.
time-name	The name of a time object in a rule validity period.
app-group-name	The name of an application group to be controlled by the rule.
comment-string	The description of a rule.

Defaults All these functions are not configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. When application access and audit is enabled, to optimize the audit records, no audit is carried out.

5. 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 Examples

1. The following example deletes all application control audit rules in the policy group policy A.

```
FS# configure terminal

FS(config)# content-policy policyA

FS(cont-plcy-config)# app-rule delete-all

FS(cont-plcy-config)# end
```

2. The following example swaps priorities of the application control audit access control rules 10 and 20 in the policy group policy A.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# app-rule priority-swap 10 20
FS(cont-plcy-config)# end
```

3. The following example adds an application control audit rule to the policy group policy A. 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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

If the configured rule-id already exists, the prompt is as follows:

```
FS(config)# app-rule 2 time-range any direction double app-group VideoAndP2PGroup action deny audit comment DenyVideoAndP2P

Rule 2 already exists, please delete it first
```

8.3 class

Use this command to add a URL class to a URL object.

class *class-name*

Use the **no** form of this command to delete a URL class from a URL object.

no class *class-name*

Parameter Description

Parameter	Description
class-name	Specifies a name of a user-defined URL class or a URL class come with the system, and allows for a maximum of 40 bytes.

Defaults

No class name is configured by default.

Command Mode

URL object configuration mode

Default Level

14

Usage Guide

1. Allow a URL object to contain a user-defined URL class and a system URL class.
2. Allow a URL object to associate an inexistent URL class.

Configuration Examples

#Add the URL class named classA to the URL object objA.

```
FS# configure terminal
FS(config)# url-object objA
FS(url-obj-config)# class classA
FS(url-obj-config)# end
```

Verification

Run the **show running-config** command to display the configuration status.

8.4 clear content-audit statistics

Use this command to clear real-time statistics of content audit.

clear content-audit statistics

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to clear real-time statistics of content audit.

Configuration Examples

#Clear real-time statistics of content audit.

```
FS#clear content-audit statistics
```

8.5 comment

Use this command to add a description of a URL class or a URL object.

comment *comment-string*

Use the **no** form of this command to delete a description of a URL class or a URL object.

no comment

Parameter Description

Parameter	Description
comment-string	Specifies a description of a URL class or a URL object, and supports a maximum of 100 characters.

Defaults

No comment string is configured by default.

Command Mode

URL object configuration mode or URL class configuration mode

Default Level

14

Usage Guide

Use this command to describe usage of a URL class or a URL object.

Configuration Examples

1. #Add a description for the URL object objA.

```
FS# configure terminal
FS(config)# url-object objA
FS(url-obj-config)# comment OBJA-COMMENT
FS(url-obj-config)# end
```

2. #Add a description for the URL class classA.

```
FS# configure terminal
FS(config)# url-class classA
FS(url-cls-config)# comment CLASSA-COMMENT
FS(url-cls-config)# end
```

Verification

Run the **show running-config** command to display the configuration status.

8.6 content-audit http-port

Use this command to add an HTTP port.

content-audit http-port *port-num*

Use the **no** form of this command to delete an HTTP port.

no content-audit http-port *port-num*

Parameter Description

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 configure or delete.

Defaults

No port number is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

When application identification is disabled, if a website needs to be audited but port 80 and port 8080 are unavailable, use this command to configure the port of the website as an HTTP port.

Configuration Examples

1. #Configure port 60000 as an HTTP port.

```
FS# configure terminal
FS(config)# content-audit http-port 60000
FS(url-obj-config)# end
```

2. #Delete port 60000 from HTTP ports.

```
FS# configure terminal
FS(config)# no content-audit http-port 60000
FS(url-obj-config)# end
```

Verification

Run the **show content-audit http-port** or **show running-config** command to display configuration information.

8.7 content-audit https-port

Use this command to add an HTTPS port.

content-audit https-port *port-num*

Use the **no** form of this command to delete an HTTPS port.

no content-audit https-port *port-num*

Parameter Description

Parameter	Description
port-num	Specifies a port ID. A value range is **1** to **65,535**. Port 443 is the default system port and is not allowed to be manually added or deleted.

Defaults

No HTTPS ports are configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

When application identification is disabled, if an HTTPS encryption website needs to be audited but port 443 is unavailable, use this command to configure the port of the website as an HTTPS port.

Configuration Examples

1. #Configure port 4430 as an HTTP port.

```
FS# configure terminal
FS(config)# content-audit https-port 4430
FS(url-obj-config)# end
```

2. #Delete port 4430 from HTTP ports.

```
FS# configure terminal
FS(config)# no content-audit https-port 4430
FS(url-obj-config)# end
```

Verification

Run the **show content-audit https-port** or **show running-config** command to display the configuration status.

8.8 content-audit write-db

Use this command to enable writing of content audit information into the local memory.

content-audit write-db { url | web-search | web-bbs | web-mail | mail | im | app-control | vid }

Use the **no** form of this command to disable writing of content audit information into the local memory.

no content-audit write-db { url | web-search | web-bbs | web-mail | mail | im | app-control | vid }

Parameter Description

Parameter	Description
N/A	N/A

Defaults

ACE series products: by default, application control audit is enabled while other functions are disabled.

Non-ACE series products: all functions are enabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

If audit information is sent to an external log server, disable saving of audit information to the local memory.

Configuration Examples

1. The following example enables writing of URL audit information into the local memory.

```
FS# configure terminal
FS(config)# content-audit write-db url
FS(url-obj-config)# end
```

2. The following example disables writing of URL audit information into the local memory.

```
FS# configure terminal
FS(config)# no content-audit write-db url
FS(url-obj-config)# end
```

Verification

Run the **show content-audit write-db/show running-config** command to display configuration information.

8.9 content-audit alarm

Use this command to enable content audit alarm.

[**no**] **content-audit alarm enable**

Use this command to specify the alarm type.

[**no**] **content-audit alarm type** { *audit-type* | **all** }

Use this command to enable alarming by Email.

[**no**] **content-audit alarm mail enable**

Use this command to set the alarming period and start time.

content-audit alarm mail cycle *n-min*

no content-audit alarm mail cycle

Parameter Description

Parameter	Description
audit-type	Specifies an audit type, including app_ctrl, url, mail, web_mail, im, web_bbs, web_search, postfile, post, ftp, telnet.

n-min	Specifies an alarming cycle, in the range from 1 to 1440.
text	Specifies a subject for the mail. Default: Content Audit Alarm,
mail-addr	Specifies a mail address. Up to 6 mail addresses are supported.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples # Enable content audit alarming by Email.

```
FS# configure terminal
FS(config)# content-audit alarm enable
FS(config)# content-audit alarm type all
FS(config)# content-audit alarm mail enable
FS(config)# content-audit alarm mail cycle 5
FS(config)# content-audit alarm mail to xxx@126.com
```

8.10 content-object

Use this command to generate a content object and enter the content object configuration mode.

content-object *object-name*

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*

Parameter Description

Parameter	Description
object-name	Specifies a name of a content object containing 40 bytes at most.

Defaults No content object is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to configure a content subject whose volume is 100.

Configuration Examples

Configure the content object objA.

Configure the keyword hello.

Configure the regular match **.ietf.org**.

```
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)# end
```

Verification

Run the **show running-config** command to display the configuration status.

8.11 content-policy

Use this command to specify a name of a content audit policy group, and enter the content audit policy group configuration mode.

content-policy *policy-name*

Use the **no** form of this command to delete a content audit policy group and all rules contained therein.

no content-policy *policy-name*

Parameter Description

Parameter	Description
policy-name	Specifies a name of a content audit policy group, and allows for a maximum of 100 bytes.

Defaults

No policy name is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to configure a policy group. One policy group supports 100 members at most.

Configuration Examples

#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.

8.12 content-policy-config

Use this command to disable all user-defined policy groups.

content-policy-config disable-all

Use the **no** form of this command to cancel disabling of all policy groups.

no content-policy-config disable-all

Use this command to disable a certain policy group.

content-policy-config disable-policy *policy-name*

Use the **no** form of this command to cancel disabling of a certain policy group.

no content-policy-config disable-policy *policy-name*

Use this command to swap priorities of two policy groups.

content-policy-config priority-swap *policy-name1 policy-name2*

Parameter Description

Parameter	Description
policy-name	Specifies a name of a content audit policy group.
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.

Defaults

All policy groups are enabled by default.

A specific policy group is enabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1. Global disabling is valid only to user-defined policy groups and is invalid to system policy groups.
2. 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.
3. Running the policy group disabling command will not delete the association between policy group content and a user.
4. When the policy group disabling command is configured, this command is invalid when a specified policy group name does not exist.
5. After a policy group is deleted, a configuration for disabling the policy group will also be deleted at the same time.
6. After performing a configuration for swapping priorities of two policy groups, run the **show running-config** command to display a change in priority ranks of the two policy groups. Output of the **show running-config** command does not display the priority swap command.

Configuration Examples

1. #Disable all user-defined policy groups.

```
FS# configure terminal
FS(config)# content-policy-config disable-all
FS(config)# end
```

2. #Disable the content audit policy group policyA.

```
FS# configure terminal
FS(config)# content-policy-config disable-policy policyA
FS(config)# end
```

3. #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.

8.13 content-policy-relate

Use this command to quit inheriting policies of a parent user group.

content-policy-relate no-inherit { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } }

Use the **no** form of this command to restore a policy inheritance attribute of a user.

no content-policy-relate no-inherit { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } }

Use this command to associate a policy group to a user.

content-policy-relate relate { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } **policy** *policy-name*

Use the **no** form of this command to delete an association between a user and a policy group.

no content-policy-relate relate { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } **policy** *policy-name*

Parameter Description

Parameter	Description
subs-name1	Static user associated with a policy group
subs-name2	Authenticated user associated with a policy group
policy-name	Policy group name

Defaults Policies of a parent user group are inherited by default.

A policy group is not associated with a user by default.

Command Mode

Global configuration mode

Default Level

14

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. During rule association, if a policy group name does not exist, the association operation is invalid and this command does not exist.

3. 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.

4. 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.

Configuration Examples

1. #Enable the static user user1 not to inherit policies of its parent user group.

```
FS# configure terminal

FS(config)# content-policy-relate no-inherit subscriber user1

FS(config)# end
```

2. #Associate the content audit policy group policyA with the static users user1 and user2, and associate policyA and policyB with the authenticated user auth-user3. And associate the policy group policy with the customized user group cstm_grp1.

```
FS# configure terminal

FS(config)# content-policy-relate relate subscriber usr1,user2 policy policyA

FS(config)# content-policy-relate relate auth-subscriber auth-user3 policy policyA,policy

FS(config)# content-policy-relate relate subscriber cstm_grp1 policy policyC

FS(config)# end
```

Verification

Run the **show running-config** command to display the configuration status.

8.14 https-audit enable

Use this command to enable HTTPS audit.

https-audit enable

Use the **no** form of this command to restore the default setting.

no https-audit enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command together with audit rules of sub-services. For example, domain names of HTTPS encrypted websites are audited and filtered after HTTPS audit is enabled and URL rules are configured.

Configuration Examples

1. #Enable HTTPS audit.

```
FS# configure terminal
FS(config)# https-audit enable
FS(config)# end
```

Verification Run the **show running-config** command to display configuration status.

Platform Description

8.15 im-rule

Use this command to enable IM default audit.

im-rule audit-default-enable

Use the **no** form of this command to disable IM default audit.

no im-rule audit-default-enable

Use this command to delete all IM rules in a policy group.

im-rule delete-all

Use this command to swap priorities of IM rules.

im-rule priority-swap *rule-id1 rule-id2*

Use this command to configure common part in an IM rule.

im-rule *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Use this command to configure description of an IM rule.

im-rule *rule-id* **im-type** *im-name* [**relation** { **and** | **or** } [**account** *content-object-name1*] [**message** *content-object-name2*]]

Use this command to delete an IM rule.

no im-rule *rule-id*

Parameter Description

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.
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.
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.

Defaults No IM rules are configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. 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.)

5. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.

6. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable IM default audit.

```
FS# configure terminal

FS(config)# content-policy _AUDIT_DEFAULT

FS(cont-plcy-config)# im-rule audit-default-enable

FS(cont-plcy-config)# end
```

2. #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
```

3. #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
```

4. #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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

1. If the configured rule ID already exists, the prompt is as follows:

```
FS(config)# im-rule 2 time-range any action permit audit comment PermitUserAMSN

Rule 2 already exists, please delete it first
```

2. If description of an IM rule is configured before the common part, the prompt is as follows:

```
FS(config)# im-rule 2 im-type msn relation or account accountA message keyA
Rule 2 is not exist
```

8.16 keyword

Use this command to add a keyword to a content object.

keyword *string*

Use the **no** form of this command to delete a keyword.

no keyword *string*

Parameter Description

Parameter	Description
string	Specifies a keyword carried in a content object. Up to 100 bytes are supported.

Defaults No key word is configured by default.

Command Mode Content object configuration mode

Default Level 14

Usage Guide Use this command to add a keyword to a content object.

Configuration Examples

1. # Configure the content object objA.
   Configure the keyword hello.

```
FS# configure terminal
FS(config)# content-object objA
FS(content-obj-config)# keyword hello
FS(content-obj-config)# end
```

Verification Run the **show running-config** command to display the configuration status.

8.17 mail-rule

Use this command to configure mail default audit.

mail-rule audit-default-enable

Use the **no** form of this command to disable mail default audit.

no mail-rule audit-default-enable

Use this command to delete all mail rules in a policy group.

mail-rule delete-all

Use this command to swap priorities of mail rules.

mail-rule priority-swap *rule-id1 rule-id2*

Use this command to configure common part in a mail rule.

mail-rule *rule-id* **time-range** *time-name* [**direction** { **in** | **out** | **double** }] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Use this command to configure description of a mail rule.

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*]

Use this command to delete a mail rule.

No mail-rule *rule-id*

Parameter Description

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.
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-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.

Defaults No mail rules are configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. When a rule is set to blocking, only the OR relation is valid.
5. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.

6. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable mail default audit.

```
FS# configure terminal

FS(config)# content-policy _AUDIT_DEFAULT

FS(cont-plcy-config)# mail-rule audit-default-enable

FS(cont-plcy-config)# end
```

2. #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
```

3. #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
```

4. #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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

1. If the configured rule ID already exists, the prompt is as follows:

```
FS(config)# mail-rule 1 time-range any action permit audit comment mail-audit-1
Rule 1 already exists, please delete it first
```

2. If description of an IM rule is configured before the common part, the prompt is as follows:

```
FS(config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000
Rule 1 is not exist
```

8.18 plugin-rule

Use this command to enable the default audit function for QQ chat records.

plugin-rule audit-default-enable

Use the **no** form of this command to disable the default audit function for QQ chat records.

no plugin-rule audit-default-enable

Use this command to enable the audit function for received QQ group chat messages.

plugin-grp-audit enable

Use the **no** form of this command to disable the audit function for received QQ group chat messages.

no plugin-grp-audit enable

Use this command to set the protocol and port ID for downloading a plug-in to a client.

plugin-config set-download-protol protol *protolname* **port** *portnum*

Use this command to set the URL for downloading a plug-in to a client.

plugin-config set-download-url *urlstring*

Use this command to delete all QQ chat message rules (plug-in rules) from a policy group.

plugin-rule delete-all

Use this command to swap priorities of plug-in access control rules.

plugin-rule priority-swap *rule-id1 rule-id2*

Use this command to add a plug-in access control rule to a content audit policy group.

plugin-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Use the **no** form of this command to delete a plug-in access control rule.

no plugin-rule *rule-id*

Parameter Description

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.
rule-id	Specifies the ID of a rule. The value ranges from **1** to **200** and a maximum of 200 rules are supported.
time-name	Specifies the time object name of a rule validity period.
content-object-name	Specifies the name of a content object used in a rule.
comment-string	Specifies the rule description.
protolname	Specifies the protocol (HTTP or HTTPS) used to download a plug-in from a device.
portnum	Specifies the protocol port used to download a plug-in from a device.
urlstring	Specifies the URL for downloading a plug-in.

Defaults

This command is not configured by default.

Command Mode

Content audit policy group configuration mode

Default Level

14

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. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the show running-config command to display a change in ranks of the two rules. Output of the show running-config command does not display the priority swap command.

5. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable the plug-in 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
```

2. #Delete all plug-in rules from a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# plugin-rule delete-all
FS(cont-plcy-config)# end
```

3. #Swap priorities of plug-in access control rules 10 and 20 in a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# plugin-rule priority-swap 10 20
FS(cont-plcy-config)# end
```

4. #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
```

5. #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
```

6. #Enable the audit function for received QQ group chat messages.

```
FS# configure terminal
FS(config)#content-policy _AUDIT_DEFAULT
FS(cont-plcy-config)#plugin-grp-audit enable
```

7. #Set the protocol and port ID for downloading a plug-in to a client.

```
FS# configure terminal
FS(config)# plugin-config set-download-protol protol https port 4430
```

8. #Configure a URL address for downloading a plug-in to a client.

```
FS# configure terminal
FS(config)#plugin-config Set-download-url http://192.168.1.111/download/
```

Verification Run the **show running-config** command to display the configuration status.

Prompt If a configured rule ID already exists, the prompt is as follows:

```
FS(config)# plugin-rule 2 time-range any content keyword-group action deny audit comment TEST
Rule 2 already exists, please delete it first
```

Common N/A

Errors

Platform Description This command is supported by gateways with built-in memories apart from the ACE series. It is also supported by the NBR-E series and EG2000F products.

8.19 postfile-rule

Use this command to enable the default audit function for posted files.

postfile-rule audit-default-enable

Use the **no** form of this command to disable the default audit function for posted files.

no postfile-rule audit-default-enable

Use this command to delete all rules for posted files (postfile rules) from a policy group.

postfile-rule delete-all

Use this command to swap the priorities of postfile access control rules.

postfile-rule priority-swap *rule-id1 rule-id2*

Use this command to add a postfile access control rule to a content audit policy group.

postfile-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Use the **no** form of this command to delete a postfile access control rule.

no postfile-rule *rule-id*

Parameter Description

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.
rule-id	Specifies the ID of a rule. The value ranges from **1** to **200** and a maximum of 200 rules are supported.
time-name	Specifies the time object name of a rule validity period.
content-object-name	Specifies the name of a content object used in a rule.
comment-string	Specifies the rule description.

Defaults This command is not configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.

5. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable the postfile 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
```

2. #Delete all postfile rules from a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# postfile-rule delete-all
FS(cont-plcy-config)# end
```

3. #Swap priorities of postfile access control rules 10 and 20 in a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# postfile-rule priority-swap 10 20
FS(cont-plcy-config)# end
```

4. #Add a postfile access audit rule to a content audit policy group named policyA, to filter out files that contain keywords in **keyword-group** and audit the files that contain such keywords.

```
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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

1. If a configured rule ID already exists, the prompt is as follows:

```
FS(config)# postfile-rule 2 time-range any content keyword-group action deny audit comment TEST
Rule 2 already exists, please delete it first
```

Common Errors

N/A

Platform

This command is supported by gateways with built-in memories apart from the ACE series. It is also supported by the

Description NBR-E series and EG2000F products.

8.20 post-rule

Use this command to enable the HTTP POST default audit function.

post-rule audit-default-enable

Use the **no** form of this command to disable the HTTP POST default audit function.

no post-rule audit-default-enable

Use this command to delete all HTTP POST rules (post rules) from a policy group.

post-rule delete-all

Use this command to swap priorities of POST access control rules.

post-rule priority-swap *rule-id1 rule-id2*

Use this command to add a POST access control rule to a content audit policy group.

post-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Use the **no** form of this command to delete a POST access control rule.

no post-rule *rule-id*

Parameter Description

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.
rule-id	Specifies the ID of a rule. The value ranges from **1** to **200** and a maximum of 200 rules are supported.
time-name	Specifies the time object name of a rule validity period.
content-object-name	Specifies the name of a content object used in a rule.
comment-string	Specifies the rule description.

Defaults This command is not configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.

5. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable the 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
```

2. #Delete all POST rules from a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# post-rule delete-all
FS(cont-plcy-config)# end
```

3. #Swap priorities of POST access control rules 10 and 20 in a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# post-rule priority-swap 10 20
FS(cont-plcy-config)# end
```

4. #Add a POST access audit rule to a content audit policy group named policyA, to filter out files that contain keywords in **keyword-group**, upload the files over HTTP POST, and audit such files.

```
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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

1. If a configured rule ID already exists, the prompt is as follows:

```
FS(config)# post-rule 2 time-range any content keyword-group action deny audit comment TEST
Rule 2 already exists, please delete it first
```

Common Errors

N/A

Platform Description

This command is supported by gateways with built-in memories apart from the ACE series. It is also supported by the NBR-E series and EG2000F products.

8.21 ssl-audit

Use this command to enable the audit function on applications of the encryption type.

ssl-audit enable

Use the **no** form of this command to disable the audit function on applications of the encryption type.

no ssl-audit enable

Use this command to configure the names of users whose applications of the encryption type need to be audited.

ssl-audit mode set-need-proxy

ssl-audit need-proxy subscriber *usrname*

ssl-audit need-proxy auth-subscriber *usrname*

Use this command to configure the names of users whose applications of the encryption type do not need to be audited.

ssl-audit mode set-unneed-proxy

ssl-audit unneed-proxy subscriber *usrname*

ssl-audit unneed -proxy auth-subscriber *usrname*

Use this command to clear the user list.

ssl-audit clear need-proxy

ssl-audit clear unneed -proxy

Parameter Description

Parameter	Description
usrname	Specifies the username.

Defaults This command is not configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

Usage Guide This command is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable the audit function on applications of the encryption type.

```
FS# configure terminal
FS(config)# content-policy _AUDIT_DEFAULT
FS(cont-plcy-config)# ssl-audit enable
FS(cont-plcy-config)# end
```

2. #Disable the audit function on applications of the encryption type.

```
FS# configure terminal
```

```
FS(config)# content-policy _AUDIT_DEFAULT
FS(cont-plcy-config)# no ssl-audit enable
FS(cont-plcy-config)# end
```

3. #Configure a list of users whose applications of the encryption type need to be audited.

```
FS# configure terminal
FS(config)# ssl-audit mode set-need-proxy
FS(config)# ssl-audit need-proxy subscriber test_usr
FS(config)# ssl-audit need-proxy auth-subscriber test_usr_auth
```

4. #Configure a list of users whose applications of the encryption type do not need to be audited.

```
FS# configure terminal
FS(config)# ssl-audit mode set-unneed-proxy
FS(config)# ssl-audit unneed-proxy subscriber test_usr
FS(config)# ssl-audit unneed-proxy auth-subscriber test_usr_auth
```

Verification Run the **show running-config** command to display the configuration status.

Prompt N/A

Common Errors N/A

Platform Description This command is supported by gateways with built-in memories apart from the ACE series. It is also supported by the NBR-E series and EG2000F products.

8.22 content-audit deny-stat

Use this command to enable the blocking statistics collection function for a specific IP address.

content-audit deny-stat ip { *A.B.C.D* | *X:X:X:X::X* }

Use the **no** form of this command to disable the blocking statistics collection function for a specific IP address (blocking statistics of all IP addresses are collected).

no content-audit deny-stat ip { *A.B.C.D* | *X:X:X:X::X* }

Use this command to clear real-time statistics on content audit.

clear content-audit deny-stat

Parameter Description

Parameter	Description
A.B.C.D | *X:X:X:X::X*	Specifies the IP address of a specific user.

Defaults This command is not configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1. After a specific IP address is set, only blocking statistics of this IP address are collected.
2. Only one specific IP address can be set in one time range.
3. After a specific IP address is deleted, blocking statistics of all users are collected.

Configuration Examples

1. #Enable the blocking statistics collection function for a specific IP address.

```
FS# configure terminal
FS(config)# content-audit deny-stat ip 192.168.1.2
FS(config)# end
```

2. #Disable the blocking statistics collection function for a specific IP address (blocking statistics of all IP addresses are collected).

```
FS# configure terminal
FS(config)#no content-audit deny-stat ip 192.168.1.2
FS(config)# end
```

3. #Clear real-time blocking statistics on content audit.

```
FS# clear content-audit deny-stat
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

N/A

Common Errors

N/A

Platform Description

8.23 clear content-audit deny-stat

Use this command to clear real-time statistics on the blocking records of content audit.

clear content-audit deny-stat

Parameter Description

Parameter	Description
N/A	N/A

Command

Privileged EXEC mode

Mode

Default Level 14

Usage Guide Use this command to clear real-time statistics on the blocking records of content audit.

Configuration Examples #Clear real-time statistics on the blocking records of content audit.

```
FS#clear content-audit deny-stat
```

8.24 report-function

Use this command to enable reporting.

report-function enable

Use the **no** form of this command to disable reporting.

no report-function enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples #Enable reporting.

```
FS# configure terminal
FS(config)# report-function enable
```

8.25 report-custom-config

Use this command to configure a custom report rule.

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**]

Use the **no** form of this command to delete the custom report rule.

no report-custom-config *rule-id*

Parameter Description

Parameter	Description
rule-id	Specifies a custom report rule ID.
reportname	Specifies a report name.
top-nu	Displays Ton N records.
cycle	Specifies a reporting cycle.
usr_name	Specifies a username or IP address,
alarm	Enables alarming.
mail_adds	Configures a mail address.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples

1. #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
```

2. #Delete a custom report rule.

```
FS# configure terminal
FS(config)# no report-custom-config 1
```

8.26 regexp

Use this command to add a URL regular expression to a URL object.

regexp *url-regexp*

Use the **no** form of this command to delete a URL regular expression.

no regexp *url-regexp*

Use this command to add a keyword regular expression to a content object.

regexp *regexp*

Use the **no** form of this command to delete a keyword regular expression.

no regexp *regexp*

Parameter Description

Parameter	Description
url-regexp	Specifies a URL regular expression, and supports a standard regular expression.
regexp	Specifies a keyword regular expression, and supports a standard regular expression.

Defaults

No regular expression is configured by default.

Command Mode

URL object configuration mode or content object configuration mode

Default Level

14

Usage Guide

Use this command to add a regular expression to a URL object or a content object.

Configuration Examples

1. #Add a regular expression to the URL object url-objA, to match a URL containing a keyword **ieft** from URLs.

```
FS# configure terminal
FS(config)# url-object url-objA
FS(url-obj-config)# regexp .*ieft.*
FS(url-obj-config)# end
```

2. #Configure the content object objectA that includes a keyword **hello** and a regular match **.ietf.org**.

```
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)# end
```

Verification

Run the **show running-config** command to display the configuration status.

8.27 show app-audit detail

Use this command to display 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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
app-group-name	Specifies a filter condition: name of an application group.
rule-name	Specifies a filter condition: rule name.
addr	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
integer1	Specifies the start position of the search result.
integer2	Specifies the end position of the search result.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display or export details about application control audit.

Configuration Examples

1. #Display details about UserA's application control audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show app-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA order-by time desc
start-item 1 end-item 20

====================================================================

Time: 2013-05-03 16:45:29

subscriber: /userA

auth-subscriber: any

Ip: 192.168.211.96
```

```
App: QQ

Rule: DenyQQ

Action: deny
```

Platform Description This command is supported by products with built-in memories.

8.28 show app-audit stat

Use this command to display 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**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
app-group-name	Specifies a filter condition: name of an application group.
rule-name	Specifies a filter condition: rule name.
addr	Specifies a filter condition: an IP address. Use “,” to separate different IP addresses.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to display statistics about application control audit.

Configuration Examples

1. #Display statistics about UserA's application control audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show app-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

Platform Description

This command is supported by products with built-in memories.

8.29 show content-audit http-port

Use this command to display an HTTP port.

show content-audit http-port

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display an HTTP port.

Configuration Examples

#Display an HTTP port.

```
FS#show content-audit http-port
HTTP port information in user:
80
8080
60000

HTTP port information in kernel:
80
8080
60000
```

8.30 show content-audit https-port

Use this command to display an HTTPS port.

show content-audit https-port

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display an HTTPS port.

Configuration Examples

#Display an HTTPS port.

```
FS#show content-audit https-port
HTTPS port information in user:         443    4430
HTTPS port information in kernel:     443    4430
```

Platform

.

8.31 show content-audit statistics

Use this command to display real-time statistics of content audit.

show content-audit statistics { **brief** | **counts** }

Parameter Description

Parameter	Description
brief	Displays an overview of real-time statistics of content audit. Only the latest 50 records are displayed.
stat	Displays count values of real-time statistics of content audit, including a total record quantity and a block record quantity.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display an overview and count values of real-time statistics.

Configuration Examples

1. #Display an overview of real-time statistics.

```
FS#show content-audit statistics brief
audit-totle-number:3
     id          relate-user            audit-time                    action    key-type
```

```
----------    ----------------    -------------------    ------    ----------------------------

              3    220.181.12.101        2014-02-10 00:02:50    permit    recv-mail-title: hello

              2    113.108.16.116        2014-02-09 14:26:31    permit    recv-mail-title: Forwards hello

              1    192.168.66.111        2014-02-09 14:26:08    permit    send-mail-title: Forwards hello
```

2. #Display count values of real-time statistics.

```
FS#show content-audit statistics counts


start-time: 2014-02-09 14:25:22


application control information:

      totle-num: 0

      block-num: 0


url reference host:

      totle-num: 0

      block-num: 0


web-search keyword:

      totle-num: 0

      block-num: 0


web-bbs post information:

      totle-num: 0

      block-num: 0


web-mail information:

      totle-num: 0

      block-num: 0


MSN information:

      totle-num: 0

      block-num: 0
```

```
QQ information:
    totle-num: 0
    block-num: 0

POP3 mail information:
    totle-num: 2
    block-num: 0

SMTP mail information:
    totle-num: 1
    block-num: 0
```

Platform Description

This command is supported by the EG series and the ACE series.

8.32 show content-audit write-db

Use this command to display the status of writing of content audit information into the local memory.

show content-audit write-db

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display the status of writing of content audit information into the local memory.

Configuration Examples

#Display the status of writing of content audit information into the local memory.

```
FS#show content-audit write-db
url_write_db:            1
web_search_write_db:     1
web_bbs_write_db:         1
web_mail_write_db:       1
mail_write_db:           1
im_write_db:              1
```

```
app_control_write_db:      1
```

Platform This command is supported by products with built-in memories.

8.33 show content-audit alarm

Use this command to display content audit alarming configuration.

show content-audit alarm

Use this command to display alarm records.

show content-audit alarm log [**from** *yyyy mm dd hh:mm:ss*] [**to** *yyyy mm dd hh:mm:ss*] [**type** *type-name*] [**offset** *n1*] [**limit** *n2*] [**by-auth**]

Parameter Description

Parameter	Description
yyyy mm dd hh:mm:ss	Specifies a start time and an end time.
type-name	Specifies an alarming type. including app-ctrl ,ftp, im , mail, post, postfile, telnet, url, web-bbs, web-mail, web-search.
n1	Specifies the start of the alarm records to be displayed.
n2	Specifies the number of alarm records to be displayed.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples

1. #Display content audit alarming configuration.

```
FS#show content-adudit alarm config
```

2. #Display alarm records.

```
FS#show content-adudit alarm log limit 10
```

8.34 show content-policy

Use this command to display related information about a policy group.

show content-policy [**policy** *policy-name* | **stat** policy-*name* | **all-rule**]

Parameter Description

Parameter	Description
content-policy	Displays an overview of all policy groups and all policies in the groups. This

	command ends when it runs to this parameter.
policy	Displays details of a specified policy group and all policies in the group.
stat	Displays a status of a specified policy group (information about whether the policy group exists, and an ID)
all-rule	Displays details of all policy groups and all policies in the groups according to policy group ranks.
policy-name	Specifies a name of a policy group. When this parameter is specified, policy details of the specified policy group are displayed.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to query related information about a policy group.

Configuration Examples

1. #Display an overview of all policy groups and all policies in the policy groups.

```
FS#show content-policy
content-policy _TOP_PRIORITY
(active)app-rule 200 time-range any app-group Block_Group action deny audit
(active)app-rule 197 time-range any app-group Block_Group action deny audit vpn

content-policy _AUDIT_DEFAULT
(active)url-rule audit-default-enable
(active)im-rule audit-default-enable
```

2. #Display details of a specified policy group and all policies in the group.

```
FS#show content-policy policy _AUDIT_DEFAULT
policy-type: url-rule

rule-id                 : 0
unit-id                 : 0
url-object              : any
rule->obj_id            : 0
action                  : permit
audit                   : Y
time-range              :
effective               : 1
```

```
comment                    : default_audit


-----------------------------------------------

policy-type: im-rule


rule-id                    : 0

time-range                 :

rule-type                  : msn,qq

keyword                    :

action                     : permit

audit                      : Y

effective                  : 1

comment                    : default_audit
```

3. #Display a status of a user-defined policy group (information about whether the policy group exists, and an ID).

```
FS#show content-policy stat _AUDIT_DEFAULT

exist: yes

policy_id: 1
```

4. #Display details of all policy groups and all policies in the groups.

```
FS#show content-policy all-rule

content-policy _TOP_PRIORITY

policy-type: app-rule


rule-id                    : 197

unit-id                    : 2

app-name                   : Block_Group

app-id                     : 4294967279

action                     : deny

audit                      : Y

vpn                        : Y

vip                        : N

time-range                 : any
```

```
effective                     : 1
comment                       :

rule-id                       : 200
unit-id                       : 1
app-name                      : Block_Group
app-id                        : 4294967279
action                        : deny
audit                         : Y
vpn                           : N
vip                           : N
time-range                    : any
effective                     : 1
comment                       :

------------------------------------------------

content-policy _AUDIT_DEFAULT
policy-type: url-rule

rule-id                       : 0
unit-id                       : 0
url-object                    : any
rule->obj_id                  : 0
action                        : permit
audit                         : Y
time-range                    :
effective                     : 1
comment                       : default_audit

------------------------------------------------
policy-type: im-rule

rule-id                       : 0
```

```
time-range                    :
rule-type                     : msn,qq
keyword                       :
action                        : permit
audit                         : Y
effective                     : 1
comment                       : default_audit


-----------------------------------------------
```

8.35 show content-policy-relate

Use this command to display association information between a user and a policy via a policy view.

show content-policy-relate policy-view [{ **policy** *policy-name* | { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } | **ip** *A.B.C.D* } }]

Use this command to display association information between a user and a policy via a user view.

show content-policy-relate user-view { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } | **ip** *A.B.C.D* } [**detail**]

Parameter Description

Parameter	Description
policy-name	Policy name
subs-name1	Static user name
subs-name2	Authenticated user name
A.B.C.D	IP address

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to display information about a user associated with a policy, or display information about a policy associated with a user.

Configuration Examples

1. #Display association information of the static user userA via a policy view.

```
FS#show content-policy-relate policy-view subscriber userA
policy-name: policyA
disable: off
pri: 1
```

```
effective: 1 (1/1/1)

subscriber: userB userA

auth-subscriber:
```

2. #Display association information of the static user userA via a user view.

```
FS#show content-policy-relate user-view subscriber userA

policy-name: policyA

pri: 1

disable: on

effective: 1 (1/1/1)

relation-disable: on

inherit: 0

---------------------------------------------------

policy-summary: 1/0

user-inherit: 1
```

3. #Display association information of the user whose IP address is A.B.C.D via a policy view. (This IP address is subscribed to the customized group cstm_grp1.)

```
FS#show content-policy-relate policy-view ip A.B.C.D

policy-name: policyC

disable: off

pri: 3

effective: 1 (1/1/1)

subscriber: cstm_grp1

auth-subscriber:
```

4. #Display association information of the user whose IP address is A.B.C.D via a user view.

```
FS#show content-policy-relate user-view ip A.B.C.D

policy-name: policyC

pri: 3

disable: on

effective: 1 (1/1/1)

relation-disable: on

inherit: 0
```

```
---------------------------------------------------

policy-summary: 1/0

user-inherit: 1
```

8.36 show https-audit enable

Use the command to display the status of HTTPS audit.

show https-audit enable

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use the command to display the status of HTTPS audit.

Configuration Examples

Display the status of HTTPS audit.

```
FS#show https-audit enable

{

    "code": 0,

    "msg": "",

    "data": {

        "enable": "on"

    }

}
```

Platform

8.37 show im-audit detail

Use this command to display details about IM audit.

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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
keyword	Specifies a filter condition: an account name.
account-string	Specifies a filter condition: an account name.
rule-name	Specifies a filter condition: rule name.
addr	Specifies a filter condition: an IP address. Use “,” to separate different IP addresses.
integer1	Specifies the start position of the search result.
integer2	Specifies the end position of the search result.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display or export details about IM audit.

Configuration Examples

1. #Display details about UserA’s MSN audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show im-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA type msn order-by time desc start-item 1 end-item 20
===================================================================================
==========
Time: 2013-05-03 15:45:59
App-type: msn
Sender: userA@hotmail.com
Receiver: userB@yahoo.com
```

```
Direction: out

Path: GigabitEthernet 0/5

Ip: 192.168.211.96

User: /userA

Auth-User:

Match-Rule: ruleA

Action: permit

Message: hello!

......
```

Platform Description

This command is supported by products with built-in memories.

8.38 show im-audit stat

Use this command to display statistics about IM audit.

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**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
keyword	Specifies a filter condition: an account name.
account-string	Specifies a filter condition: an account name.
rule-name	Specifies a filter condition: rule name.
addr	Specifies a filter condition: IP address of the intranet.

Command

Privileged EXEC mode

Mode

Default Level 14

Usage Guide Use this command to display statistics about IM audit.

Configuration Examples

1. #Display statistics about UserA's MSN audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show im-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA type msn

50
```

Platform Description This command is supported by products with built-in memories.

8.39 show mail-audit attachment-info

Use this command to display information about mail audit attachments.

show mail-audit attachment-info timestamp *timestamp* **rand-id** *rand-id*

Parameter Description

Parameter	**Description**
timestamp	Specifies a timestamp.
rand-id	Specifies a random ID.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use the **show mail-audit detail** command to display the timestamp and random ID of a mail, before using this command to display information about mail audit attachments.

Configuration Examples

1. #Display information about audit attachments of the mail whose timestamp is 1286849291 and random ID is 1087821567.

```
FS#show mail-audit attachment-info timestamp 1286849291 rand-id 1087821567

Size(Byte)    Path

==============================================================

80646           mnt/sata/mail/20130503/unknown(09-01-19-44-40).gif

150528          mnt/sata/mail/20130503/test-file.doc
```

Platform Description This command is supported by products with built-in memories.

8.40 show mail-audit detail

Use this command to display details about mail audit.

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*]

Parameter Description

Parameter	**Description**
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
keyword1	Specifies a filter condition: a sender keyword.
keyword2	Specifies a filter condition: a receiver keyword.
keyword3	Specifies a filter condition: a mail title keyword.
rule-name	Specifies a filter condition: rule name.
integer1	Specifies the start position of the search result.
integer2	Specifies the end position of the search result.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide

Use this command to display or export details about mail audit.

Configuration Examples

1. #Display details about UserA's mail audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show mail-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA order-by time desc start-item 1 end-item 20

================================================================================
============

Time: 2013-05-03 15:45:59

App-type: SMTP

Direction: out

Path: GigabitEthernet 0/5

Ip: 192.168.211.96

User: /userA

Auth-User:

Match-Rule: ruleA

Action: permit

Timestamp: 1287027112

Rand-id: 1686175891

From: userA@hotmail.com

To: userB@yahoo.com

Subject: hello

Body: hello

……
```

Platform Description

This command is supported by products with built-in memories apart from the ACE series.

8.41 show mail-audit stat

Use this command to display statistics about mail audit.

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**]

Parameter Description

Parameter	Description

hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
keyword1	Specifies a filter condition: a sender keyword.
keyword2	Specifies a filter condition: a receiver keyword.
keyword3	Specifies a filter condition: a mail title keyword.
rule-name	Specifies a filter condition: rule name.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display statistics about mail audit.

Configuration Examples

1. #Display statistics about UserA's mail audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show mail-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA

50
```

Platform Description

This command is supported by products with built-in memories apart from the ACE series.

8.42 show plugin-audit detail

Use this command to display details about the audit of QQ chat records.

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*] [**message** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** |

desc } [**start-item** *integer1* **end-item** *integer2*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
addr	Specifies the filter condition: IP address for exact match. IP addresses are separated by a comma (,).
keyword	Specifies the filter condition: filter keyword. Multiple keywords can be used for filtering and the keywords are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).
integer1	Specifies the start position in the search results.
integer2	Specifies the end position in the search results.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to query or export details about the audit of QQ chat records.

Configuration Examples

1. #Query details about the audit of QQ chat messages from 00:00 to 24:00 on November 29, 2016.

```
FS# show plugin-audit detail time-range from 2016 11 29 00:00:00 to 2016 11 29 23:59:59 order-by time desc
start-item 1 end-item 20
================================================================================
============
id: 157
sip: 172.21.159.221
soft: QQ
type: f
sendid: 263985410
sendname: Joe
recvid: 792941456
recvname: |Jane
```

```
datetime: 2016:11:29:18:00:43
flag: s
len: 5
message: hello
```

Prompt N/A

Platform Description This command is supported by products with built-in memories apart from the ACE series.

8.43 show plugin-audit stat

Use this command to display statistics on the audit of QQ chat records.

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*] [**message** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]

Parameter Description

Parameter	**Description**
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
addr	Specifies the filter condition: IP address for exact match. IP addresses are separated by a comma (,).
keyword	Specifies the filter condition: filter keyword. Multiple keywords can be used for filtering and the keywords are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to query statistics on the audit of QQ chat records.

Configuration Examples

1. #Query plugin audit statistics from 00:00 on May 1, 2013 to 24:00 on May 7, 2013.

```
FS# show plugin-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59
50
```

Prompt N/A

Platform Description This command is supported by products with built-in memories apart from the ACE series.

8.44 show postfile-audit detail

Use this command to display details about the audit of posted files.

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*] [**filename** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
addr	Specifies the filter condition: IP address for exact match. IP addresses are separated by a comma (,).
keyword	Specifies the filter condition: filter keyword. Multiple keywords can be used for filtering and the keywords are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).
integer1	Specifies the start position in the search results.
integer2	Specifies the end position in the search results.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to query or export details about the audit of posted files.

Configuration Examples 1. #Query details about the audit of posted files of user A from 00:00 on September 4, 2016 to 24:00 on November 4, 2016.

```
FS# show postfile-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time
desc start-item 1 end-item 20
id: 1
time_stamp: 1480056761
day_time: 2016-11-25 14:52:41
sip: 3.3.3.54
dip: 60.28.228.9
sport: 60141
dport: 80
mac_addr: f48e.388f.f50d
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
obj_name:
action: permit
username: nabi2006@sina.com
nickname:
uid:
app_type: Sina email attachment
filename: Dingdangmao.jpg
path: /mnt/sata0/file/20161125/1480056761-000000-Dingdangmao.jpg
filesize: 412871
relate_id: 03030336eaed3c1ce4090050
filetype:
……
```

Prompt N/A

Platform Description This command is supported by products with built-in memories apart from the ACE series.

8.45 show postfile-audit relate-id

Use this command to display the attachment of an email or posted file.

show postfile-audit relate-id *rand-id* **timestamp** *timestamp*

Parameter Description

Parameter	Description
relate-id	Specifies the attachment ID of an email.
timestamp	Specifies the timestamp.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Run the **show mail-audit detail** command to display the timestamp and attachment ID of an email and then run the **show postfile-audit relate-id** command to display the attachment of the email.

Configuration Examples

1. #Display the attachment of an email with **timestamp** set to **1476253284** and **relate-id** set to **03030336e7353d879e5a0050**.

```
FS#show postfile-audit relate-id 03030336e7353d879e5a0050 timestamp 1476253284
Size(Byte)      Path
==================================================
relate_id: 03030336e7353d879e5a0050
time_stamp: 1476253284
filesize: 111
path: /mnt/sata0/file/20161013/1476339684-000000-F1.jpg
```

Prompt

N/A

Platform Description

This command is supported by products with built-in memories apart from the ACE series.

8.46 show postfile-audit stat

Use this command to display statistics on the audit of posted files.

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*] [**filename** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.

hour4	Specifies the time filter condition: end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
addr	Specifies the filter condition: IP address for exact match. IP addresses are separated by a comma (,).
keyword	Specifies the filter condition: filter keyword. Multiple keywords can be used for filtering and the keywords are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to query statistics on the audit of posted files.

Configuration Examples

1. #Query statistics on the audit of posted files of user A from 00:00 on May 1, 2013 to 24:00 on May 7, 2013.

```
FS# show postfile-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

Prompt

N/A

Platform Description

This command is supported by products with built-in memories apart from the ACE series.

8.47 show post-audit detail

Use this command to display details about the POST audit.

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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.

hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
addr	Specifies the filter condition: IP address for exact match. IP addresses are separated by a comma (,).
keyword	Specifies the filter condition: filter keyword. Multiple keywords can be used for filtering and the keywords are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).
integer1	Specifies the start position in the search results.
integer2	Specifies the end position in the search results.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to query or export details about the POST audit.

Configuration Examples

1. #Query details about the POST audit of user A from 00:00 to 24:00 on November 4, 2016.

```
FS# show post-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time desc
start-item 1 end-item 20
===================================================================================
============
====================================================
id: 7
time_stamp: 1479868298
day_time: 2016-11-23 10:31:38
sip: 3.3.3.54
dip: 124.251.20.10
sport: 59199
dport: 80
mac_addr: f48e.388f.f50d
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
obj_name:
action: permit
app_type: common webpage browse
url: http://www.btime.com/
```

```
body: content[]={}
====================================================
……
```

Prompt N/A

Platform Description This command is supported by products with built-in memories apart from the ACE series.

8.48 show post-audit stat

Use this command to display statistics on the POST audit.

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**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
addr	Specifies the filter condition: IP address for exact match. IP addresses are separated by a comma (,).
keyword	Specifies the filter condition: filter keyword. Multiple keywords can be used for filtering and the keywords are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to query statistics on the POST audit.

Configuration Examples

1. #Query statistics about the POST audit of user A from 00:00 to 24:00 on November 4, 2016.

```
FS# show post-audit stat time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA
1508
```

Prompt

N/A

Platform Description

This command is supported by products with built-in memories apart from the ACE series.

8.49 show content-audit deny-stat

Use this command to display the real-time blocking statistics of content audit.

show content-audit deny-stat { brief | counts | ip}

Parameter Description

Parameter	Description
brief	Displays the summary of real-time blocking statistics of content audit. Only recent 50 records are displayed.
counts	Displays the counts in real-time blocking statistics of content audit, including the total record count and blocking record count.
ip	Displays the blocking statistics of a specific IP address.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display the summary of and counts in the real-time blocking statistics.

Configuration Examples

1. #Display the summary of real-time blocking statistics.

```
FS#show content-audit deny-stat brief
audit-totle-number:1
    id          relate-user         audit-time        ca_type        app_type           plcy_name
content
---------- ---------------- ---------------- ---------- ---------------- ---------------- ----------------------------
         1 10                   2017-10-10 10:28:24 IM          QQ                 _TOP_PRIORITY      QQ:
263985410 LOGIN
```

2. #Display the counts in real-time blocking statistics.

```

FS#show content-audit statistics counts

start-time: 2017-10-10 10:28:15

```

```
application control information:
    totle-num: 0
    block-num: 0

url reference host:
    totle-num: 0
    block-num: 0

web-search keyword:
    totle-num: 0
    block-num: 0

web-bbs post information:
    totle-num: 0
    block-num: 0

web-mail information:
    totle-num: 0
    block-num: 0

MSN information:
    totle-num: 0
    block-num: 0

QQ information:
    totle-num: 1
    block-num: 1

POP3 mail information:
    totle-num: 0
    block-num: 0

SMTP mail information:
    totle-num: 0
    block-num: 0

virtual id information:
    totle-num: 0
    block-num: 0

postfile information:
    totle-num: 0
    block-num: 0
```

```
post information:
       totle-num: 0
       block-num: 0

plugin information:
       totle-num: 0
       block-num: 0
```

3. #Display the configured IP address.

```
FS# show content-audit deny-stat ip
content-audit deny-stat ip 192.168.1.2
```

Prompt N/A

Platform Description This command is supported by all gateway series.

8.50 show url-audit detail

Use this command to display details about URL audit.

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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use “,” to separate different IP addresses.
class-name	Specifies a filter condition: a name of a designated system

	class, supporting exact matching.
obj-name	Specifies a filter condition: a name of a URL object, supporting mode matching.
url-string	Specifies a filter condition: a URL string, supporting mode matching.
host-string1	Specifies a filter condition: a HOST string, supporting exact matching.
host-string2	Specifies a filter condition: a HOST site, supporting exact matching.
integer1	Specifies the start position of the search result.
integer2	Specifies the end position of the search result.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display or export details about URL audit.

Configuration Examples

1. #Display details about UserA's URL audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show url-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA order-by time desc
start-item 1 end-item 20
================================================================================
============
Time: 2013-05-03 15:45:59
Ip: 192.168.211.96
Subscriber: /userA
Auth-subscriber:
Match-rule: ruleA
Action: permit
URL: http://www.ietf.org/
URL-class: overseas website
……
```

Platform Description

This command is supported by products with built-in memories.

8.51 show url-audit stat

Use this command to display statistics about url audit.

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**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
class-name	Specifies a filter condition: a name of a designated system class, supporting exact matching.
obj-name	Specifies a filter condition: a name of a URL object, supporting mode matching.
host-string	Specifies a filter condition: a HOST site, supporting exact matching.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display statistics about URL audit.

Configuration Examples

1. #Display statistics about UserA's URL audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show url-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
500
```

Platform Description

This command is supported by products with built-in memories.

8.52 show url-audit top

Use this command to display Top N of most visited URL websites.

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**]

Parameter Description

Parameter	**Description**
n	Specifies Top N, ranging from 1 to 100.
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
class-name	Specifies a filter condition: a name of a designated system class, supporting exact matching.
obj-name	Specifies a filter condition: a name of a URL object, supporting mode matching.
host-string	Specifies a filter condition: a HOST site, supporting exact matching.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display or export Top N of most visited URL websites.

Configuration Examples

1. #Display Top2 most visited websites within 24 hours.

```
FS# show url-audit top 2 recent 24
HOST                     Times              url-class                  url-object
=============================================================
www.ietf.org               32349              class1             obj1
www.w3c.org                  30032              class2             obj2
```

Platform Description

This command is supported by products with built-in memories.

8.53 show url-class system

Use this command to display names of classes in the current URL library of the system.

show url-class system [**class** { **id** *class-id* | **name** *class-name* }]

Use this command to display description information of the current URL library of the system.

show url-class system comment [**class** { **id** *class-id* | **name** *class-name* }]

Use this command to display current user-defined information of the URL library of the system.

show url-class system custom [**class** { **id** *class-id* | **name** *class-name* }]

Use this command to display related information about the exact filtering library.

show url-class system exact

Parameter Description

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

Default Level

14

Usage Guide

Use this command to display related information about a system URL library.

Configuration Examples

1. #Display names of classes in the current URL library of the system.

```
FS# show url-class system
```

```
version-1.0

2010-4-22

system-url-class-number: 32

Class 1

    Job recruitment

    IT class

    Web communication

    Force

    Virus

Class 2

    Science

    Adult

    ...
```

2. #Display group and class information of the current URL library of the system.

```
FS# show url-class system custom

version-1.0

2010-4-22

system-url-class-number:32

consumption-amount:2

remain-amount:998 (necessary statistics)

Class 1

    url-class: Job recruitment

        comment: Job recruitment class description

           add: add1.com

           add: add2.com

          move: move1.com

          move: move2.com

    url-class: Military

        comment: Military class description

    url-class: IT class

        comment: IT class description

           add: add1.com

           add: add2.com
          move: move1.com

          move: move2.com

Class 2

    url-class:

        comment:

    ...
```

3. #Display class and description information of the current URL library of the system.

```
FS# show url-class system comment

version-1.0

2010-4-22

System url class number: 32

Class 1

    Job recruitment: description 1

    IT class: description 2

    Web communication: description 3

…
```

4. #Display related information about the exact filtering library.

```
FS# show url-class system exact

exact-filter: disable
```

8.54 show url-class url

Use this command to display a system URL class to which a designated URL string belongs, and the currently configured URL class.

show url-class url *url-string*

Parameter Description

Parameter	**Description**
url-string	String representing a URL

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display a system URL class to which a designated URL string belongs, and the currently configured URL class.

Configuration Examples

#Display class information of the URL **FS.com.cn**.

```
FS# show url-class url FS.com.cn
url:FS.com.cn
default-system-class: business
modified-system-class:
custom-class:test1
```

8.55 show url-class user-cfg

Use this command to display configuration information of a user-defined URL class.

show url-class user-cfg [*class-name*]

Parameter Description

Parameter	Description
class-name	Name of a user-defined class

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display configuration information of a user-defined URL class.

Configuration Examples

1. #Display configuration information of each user-defined URL class.

```
FS# show url-class user-cfg
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
url-class:CLASSB
url:w3c.org
comment:comment for CLASSB
```

2. #Display configuration information of a designated user-defined URL class.

```
FS# show url-class user-cfg CLASSA
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
```

8.56 show vid-audit detail

Use this command to display virtual identity audit.

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*]

Parameter Description

Parameter	**Description**
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
uid-string	Specifies a filter condition: UID.
nick-string	Specifies a filter condition: nick name.
addr 1	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
addr 2	Specifies a filter condition: a MAC address. Use "," to separate different IP addresses.
integer1	Specifies the start position of the search result.
integer2	Specifies the end position of the search result.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display or export virtual identity audit.

Configuration Examples

#Display details about UserA's virtual identity audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show vid-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA type msn order-by time desc start-item 1 end-item 20
==========================================================================================
=============
day_time: 2013-05-03 15:45:59
internal_ip: 192.168.211.96
mac_addr: 00d0.1234.abcd
usr_grp: /
usr_name: /userA
vid_type: wechat
vid_action: LOGOUT
uid: 1755006665
nick_name:
……
```

8.57 show vid-audit stat

Use this command to display virtual identity audit statistics.

show vid-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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
uid-string	Specifies a filter condition: UID.
nick-string	Specifies a filter condition: nick name.
addr 1	Specifies a filter condition: an IP address. Use “,” to separate different IP addresses.
addr 2	Specifies a filter condition: a MAC address. Use “,” to separate different IP addresses.

Command Privileged EXEC mode

Mode

Default Level 14

Usage Guide Use this command to display virtual identity audit statistics.

Configuration Examples

#Display statistics about UserA's virtual identity audit from 0:0:0 May 1st, 2013 to 23:59:59 May 7th, 2013.

```
FS# show vid-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA type msn

50
```

Platform Description This command is supported by products with built-in memories apart from the ACE series.

8.58 show web-bbs-audit detail

Use this command to display 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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
keyword	Specifies a filter condition
rule-name	Specifies a filter condition: a rule name.
integer1	Specifies the start position of the search result.
Integer2	Specifies the end position of the search result.

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Examples #Display Web BBS audit details of user A from 2013-5-1 0:00 to 2013-5-7 24:00.

```
FS# show web-bbs-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA order-by time desc start-item 1 end-item 20
======================================================================
Time: 2013-05-03 16:45:29
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
Rule: ruleA
Action: permit
Title: hello
Body: hello
```

8.59 show web-bbs-audit stat

Use this command to display 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**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.

addr	Specifies a filter condition: an IP address. Use “,” to separate different IP addresses.
keyword	Specifies a filter condition
rule-name	Specifies a filter condition: a rule name.

Defaults

Command Mode Priviledge EXEC mode

Default Level 14

Usage Guide N/A

Configuration Examples #Display Web BBS audit statistics of user A from 2013-5-1 0:00 to 2013-5-7 24:00.

```
FS# show web-bbs-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

8.60 show web-mail-audit attachment-info

Use this command to displays information about Web mail attachments.

show web-mail-audit attachment-info timestamp *timestamp* **rand-id** *rand-id*

Parameter Description

Parameter	Description
timestamp	Timestamp
rand-id	Random ID

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Examples #Display Web mail attachments with timestamp 1286849291 and random ID 1087821567.

```
FS#show web-mail-audit attachment-info timestamp 1286849291 rand-id 1087821567
Size(Byte)    Path
==============================================================
80646         mnt/sata/mail/20130503/unknown(09-01-19-44-40).gif
150528        mnt/sata/mail/20130503/test-file.doc
```

The following example disables

8.61 show web-mail-audit detail

Use this command to display 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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
keyword1	Specifies a filter condition: a sender keyword.
keyword2	Specifies a filter condition: a receiver keyword.
keyword3	Specifies a filter condition: a mail subject keyword.
rule-name	Specifies a filter condition: a rule name.
integer1	Specifies the start position of the search result.
integer2	Specifies the end position of the search result.

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration #Display Web mail audit details of user A from 2013-5-1 0:00 to 2013-5-7 24;00.

Examples

```
FS# show web-mail-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA order-by time
desc start-item 1 end-item 20
================================================================================
============
Time: 2013-05-03 15:45:59
Direction: out
Path: GigabitEthernet 0/5
Ip: 192.168.211.96
User: /userA
Auth-User:
Match-Rule: ruleA
Action: permit
Timestamp: 1287027112
Rand-id: 1686175891
From: userA@hotmail.com
To: userB@yahoo.com
Subject: hello
Body: hello
```

8.62 show web-mail-audit stat

Use this command to display 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**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use “,” to separate different IP addresses.
keyword1	Specifies a filter condition: a sender keyword.
keyword2	Specifies a filter condition: a receiver keyword.
keyword3	Specifies a filter condition: a mail title keyword.

rule-name	Specifies a filter condition: rule name.

Defaults N/A

Command Mode Priviledges EXEC mode

Default Level 14

Usage Guide N/A

Configuration Examples #Display Web mail audit statistics of user A from 2013-5-1 0:00 to 2013-5-7 24;00.

```
FS# show web-mail-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

8.63 show web-search-audit detail

Use this command to 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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.
subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use “,” to separate different IP addresses.
keyword	Specifies a filter condition
rule-name	Specifies a filter condition: a rule name.
integer1	Specifies the start position of the search result.
Integer2	Specifies the end position of the search result.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples #Display Web search audit details of user A from 2013-5-1 0:00 to 2013-5-7 24:00.

```
FS# show web-search-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA order-by time desc start-item 1 end-item 20
======================================================================
Time: 2013-05-03 16:45:29
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
Rule: ruleA
Action: permit
URL: http://www.baidu.com/s?ie=utf-8&bs=hello&rsv_bp=1&rsv_spt=3&wd=hello
search-word: hello
```

8.64 show web-search-audit stat

Use this command to display 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**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies year, month and day.
hh:mm:ss	Specifies hour, minute and second.
hour1	Specifies time filter condition: the start hour.
hour2	Specifies time filter condition: the end hour.
hour3	Specifies time filter condition: the start hour.
hour4	Specifies time filter condition: the end hour.
intf-name	Specifies an interface name.
bridge-num	Specifies a bridge number.
subs-name1	Specifies a filter condition: static username, supporting exact match.

subs-name2	Specifies a filter condition: authentication username, supporting exact match.
addr	Specifies a filter condition: an IP address. Use "," to separate different IP addresses.
keyword	Specifies a filter condition
rule-name	Specifies a filter condition: a rule name.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples #Display Web search audit statistics of user A from 2013-5-1 0:00 to 2013-5-7 24:00.

```
FS# show web-search-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

8.65 url

Use this command to add a URL entry to a URL class.

url *url-string*

Use the **no** form of this command to delete a URL entry.

no url *url-string*

Parameter Description

Parameter	Description
url-string	Specifies a URL entry 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**.

Defaults No URL string is configured by default.

Command Mode URL class configuration mode

Default Level 14

Usage Guide 1. The URL mode matching currently supports only 2 levels of directories. The user configuration **ietf.org/2006/12/1** is not allowed.
2. The URL sub domain name mode matching currently supports only 4 levels of sub domain names. If the user configuration is **test.rfc.download.ietf.org**, only an exact domain name can be matched.

Configuration Examples #Add the entry **ietf.org** to the URL class classA.

```
FS# configure terminal
FS(config)# url-class classA
FS(url-cls-config)# url ietf.org
FS(url-cls-config)#end
```

Verification Run the **show running-config** command to display the configuration status.

Prompt Information If the configured URL format is incorrect, the following prompt information is displayed:

```
FS(config)# url ietf.org/2006/12/1
Format error
```

8.66 url-audit

Use this command to enable the corresponding URL optimization audit function.
url-audit { **exact-filter** | **except-postfix** | **except-regexp** [*regexp*] | **only-get** | **optimize-cache** [*time*] }

Use the **no** form of this command to disable the corresponding URL optimization audit function.
no url-audit { **exact-filter** | **except-postfix** | **except-regexp** [*regexp*] | **only-get** | **optimize-cache** [*time*] }

Parameter Description

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.

Defaults This function is enabled by default. The command is not displayed, and is displayed only after the **no** form of this command is run.

Command Mode Global configuration mode

Default Level 14

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.

Configuration Examples

1. #Audit only an HTTP GET operation.

```
FS# configure terminal
FS(config)# url-audit only-get
FS(config)#end
```

2. #Quit auditing a URL that meets the default regular expression (**.*=.*&.*=.***):

```
FS# configure terminal
FS(config)# url-audit except-regexp
FS(config)# end
```

3. #Quit auditing a URL with a suffix of a picture:

```
FS# configure terminal
FS(config)# url-audit except-postfix
FS(config)# end
```

4. #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
```

Verification

Run the **show running-config** command to display the configuration status.

8.67 url-class

Use this command to specify a name of a URL class and enter the URL class configuration mode.
url-class *class-name*

Use the **no** form of this command to delete a URL class.
no url-class *class-name*

Parameter Description

Parameter	Description

class-name	Name of a URL class

Defaults No URL class is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to configure a URL class.

Configuration Examples #Add the URL class classA.

```
FS# configure terminal
FS(config)# url-class classA
FS(url-obj-config)#end
```

Verification Run the **show running-config** command to display the configuration status.

8.68 url-filter-notice

Use this command to configure content to be displayed on a URL filtering prompt page.

url-filter-notice display [*text*]

Use the **no** form of this command to disable the display function of a URL filtering prompt page.

no url-filter-notice

Parameter Description

Parameter	Description
text	Specifies information to be displayed on a URL filtering prompt page. Default information is displayed if this parameter is not specified.

Defaults This display function is enabled by default. Default content to be displayed is as follows:
"You are forbidden to visit the website, please contact webmaster!"

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to configure content to be displayed on a URL filtering prompt page.

Configuration Examples #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.

8.69 url-object

Use this command to specify a name of a URL object and enter the URL object configuration mode.

url-object *object-name*

Use the **no** form of this command to delete a URL object.

no url-object *object -name*

Parameter Description

Parameter	Description
object-name	Specifies a name of a URL object, and allows for a maximum of 40 bytes.

Defaults No URL object is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to configure a URL object. 100 URL objects are supported.

Configuration Examples #Add the URL object objA.

```
FS# configure terminal
FS(config)# url-object objA
FS(url-obj-config)# end
```

Verification Run the **show running-config** command to display the configuration status.

8.70 url-redirect-rule

Use this command to delete all URL redirection rules in a policy group.

url-redirect-rule delete-all

Use this command to swap priorities of URL redirection access control rules.

url-redirect-rule priority-swap *rule-id1 rule-id2*

Use this command to add a URL redirection access control rule to a content audit policy group.

url-redirect-rule *rule-id* **time-range** *time-name* **from** *url-1* **to** *url-2* [**comment** *comment-string*]

Use the **no** form of this command to delete a URL redirection access control rule.

no url-redirect-rule *rule-id*

Parameter Description

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.
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	Specifies the URL address to be redirected.
url-2	Specifies the URL address that is redirected to.
comment-string	Specifies a description of a rule.

Defaults The Web search rule function is disabled by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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 associated with the rule does not exist.
4. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.

Configuration Examples

1. #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
```

2. #Swap priorities of the URL redirection access control rule 10 and the URL redirection access control rule 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
```

3. #Add a URL redirection access audit rule to the content audit policy group policyA: redirect 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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt Information

1. If the configured rule ID already exists, the following prompt information is displayed:

```
FS(config)# url-redirect-rule 2 time-range any from www.sina.com.cn to www.FS.com.cn comment sina-redirect

Rule 2 already exists, please delete it first
```

8.71 telnet-rule

Use this command to enable the Telnet default audit function.

telnet-rule audit-default-enable

Use the **no** form of this command to disable the Telnet default audit function.

no telnet-rule audit-default-enable

Use this command to delete all Telnet rules from a policy group.

telnet-rule delete-all

Use this command to swap priorities of Telnet access control rules.

telnet-rule priority-swap *rule-id1 rule-id2*

Use this command to add a Telnet access control rule to a content audit policy group.

telnet-rule *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Use the **no** form of this command to delete a Telnet access control rule.

no telnet-rule *rule-id*

Parameter Description

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.
rule-id	Specifies the ID of a rule. The value ranges from **1** to **200** and a maximum of 200 rules are supported.
time-name	Specifies the time object name of a rule validity period.
comment-string	Specifies the rule description.

Defaults This command is not configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.
5. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #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
```

2. #Delete all Telnet rules from a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# telnet-rule delete-all
FS(cont-plcy-config)# end
```

3. #Swap priorities of Telnet access control rules 10 and 20 in a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# telnet-rule priority-swap 10 20
FS(cont-plcy-config)# end
```

4. #Add a Telnet access audit rule to a content audit policy group named policyA, to filter Telnet behaviors and audit the Telnet behaviors that are filtered out.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# telnet-rule 2 time-range any action deny audit comment TEST
FS(cont-plcy-config)# end
```

Verification Run the **show running-config** command to display the configuration status.

Prompt 1. If a configured rule ID already exists, the prompt is as follows:

```
FS(config)# telnet-rule 2 time-range any action deny audit comment TEST
Rule 2 already exists, please delete it first
```

Common Errors N/A

Platform Description This command is supported by gateways with built-in memories apart from the ACE series. It is also supported by the NBR-E series and EG2000F products.

8.72 ftp-rule

Use this command to enable the FTP default audit function.

ftp-rule audit-default-enable

Use the **no** form of this command to disable the FTP default audit function.

no ftp-rule audit-default-enable

Use this command to delete all FTP rules from a policy group.

ftp-rule delete-all

Use this command to swap priorities of FTP access control rules.

ftp-rule priority-swap *rule-id1 rule-id2*

Use this command to add an FTP access control rule to a content audit policy group.

ftp-rule *rule-id* **time-range** *time-name* [**filename** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Use the **no** form of this command to delete an FTP access control rule.

no ftp-rule *rule-id*

Use this command to enable/disable the audit of files uploaded over FTP.

[**no**] **ftp-upload-file-audit enable**

Parameter Description

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.
rule-id	Specifies the ID of a rule. The value ranges from **1** to **200** and a maximum of 200 rules are supported.
time-name	Specifies the time object name of a rule validity period.
content-object-name	Specifies an object that an FTP filename needs to match.
comment-string	Specifies the rule description.

Defaults This command is not configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.

5. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples 1. #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
```

2. #Delete all FTP rules from a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# ftp-rule delete-all
FS(cont-plcy-config)# end
```

3. #Swap priorities of FTP access control rules 10 and 20 in a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# ftp-rule priority-swap 10 20
FS(cont-plcy-config)# end
```

4. #Add an FTP audit rule to a content audit policy group named policyA, to filter out files that contain keywords in **keyword-group** and audit such files.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# ftp-rule 2 time-range any filename keyword-group action deny audit comment TEST
FS(cont-plcy-config)# end
```

5. #Enable the audit on files uploaded over FTP.

```
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.

Prompt 1. If a configured rule ID already exists, the prompt is as follows:

```
FS(config)# ftp-rule 2 time-range any action deny audit comment TEST
Rule 2 already exists, please delete it first
```

Common Errors N/A

Platform Description This command is supported by gateways with built-in memories apart from the ACE series. It is also supported by the NBR-E series and EG2000F products.

8.73 show telnet-audit detail

Use this command to display details about the Telnet audit.

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*]

Parameter Description

Parameter	**Description**
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
addr1	Specifies the filter condition: intranet IP address for exact match. IP addresses are separated by a comma (,).

addr2	Specifies the filter condition: server IP address for exact match. IP addresses are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).
integer1	Specifies the start position in the search results.
integer2	Specifies the end position in the search results.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to query or export details about the Telnet audit.

Configuration Examples 1. #Query details about the Telnet audit of user A from 00:00 on September 4, 2016 to 24:00 on November 4, 2016.

```
FS# show telnet-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time desc start-item 1 end-item 20
id: 1
time_stamp: 1480056761
day_time: 2016-11-25 14:52:41
sip: 3.3.3.54
dip: 60.28.228.9
sport: 60141
dport: 23
mac_addr: f48e.388f.f50d
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
app_type: telnet
state:connect
……
```

Prompt N/A

Platform Description This command is supported by products with built-in memories apart from the ACE series.

8.74 show telnet-audit stat

Use this command to display statistics on the Telnet audit.

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]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
addr1	Specifies the filter condition: IP address for exact match. IP addresses are separated by a comma (,).
addr2	Specifies the filter condition: server IP address for exact match. IP addresses are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to query statistics on the Telnet audit.

Configuration Examples

1. #Query statistics on the Telnet audit of user A from 00:00 on May 1, 2013 to 24:00 on May 7, 2013.

```
FS# show telnet-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

Prompt

N/A

Platform Description

This command is supported by products with built-in memories apart from the ACE series.

8.75 show ftp-audit detail

Use this command to display details about the FTP audit.

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** *addr1*] [**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*]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
keyword	Specifies the filter condition: file name keyword. Multiple keywords can be used for filtering and the keywords are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).
addr1	Specifies the filter condition: intranet IP address for exact match. IP addresses are separated by a comma (,).
integer1	Specifies the start position in the search results.
integer2	Specifies the end position in the search results.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to query or export details about the FTP audit.

Configuration Examples

1. #Query details about the FTP audit of user A from 00:00 on September 4, 2016 to 24:00 on November 4, 2016.

```
FS# show ftp-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time desc
start-item 1 end-item 20
id: 1
time_stamp: 1480056761
day_time: 2016-11-25 14:52:41
sip: 3.3.3.54
dip: 60.28.228.9
sport: 60141
dport: 21
mac_addr: f48e.388f.f50d
file name:aaa.txt
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
state:upload
```

```
action:permit
```

Prompt N/A

Platform Description This command is supported by products with built-in memories apart from the ACE series.

8.76 show ftp-audit stat

Use this command to display statistics on the FTP audit.

show ftp-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*] [**file-name** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]

Parameter Description

Parameter	Description
hours	Specifies recent hours.
yyyy mm dd	Specifies the year, month, and day.
hh:mm:ss	Specifies the hour, minute, and second.
hour1	Specifies the time filter condition: start hour.
hour2	Specifies the time filter condition: end hour.
hour3	Specifies the time filter condition: start hour.
hour4	Specifies the time filter condition: end hour.
subs-name1	Specifies the filter condition: static username for exact match.
subs-name2	Specifies the filter condition: authenticated username for exact match.
addr1	Specifies the filter condition: intranet IP address for exact match. IP addresses are separated by a comma (,).
keyword	Specifies the filter condition: file name keyword. Multiple keywords can be used for filtering and the keywords are separated by a comma (,).
rule-name	Specifies the filter condition: rule name. Multiple rule names can be used for filtering and the rule names are separated by a comma (,).

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Use this command to query statistics on the FTP audit.

Configuration Examples 1. #Query statistics on the FTP audit of user A from 00:00 on May 1, 2013 to 24:00 on May 7, 2013.

```
FS# show ftp-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

Prompt N/A

Platform Description This command is supported by products with built-in memories apart from the ACE series.

8.77 file-rule

Use this command to delete all file rules from a policy group.

file-rule delete-all

Use this command to swap priorities of file access control rules.

file-rule priority-swap *rule-id1 rule-id2*

Use this command to add a file access control rule to a content audit policy group.

file-rule *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

file-rule *rule-id* **relation** { **and** | **or** } [**file-name** *content-obj-string1*] [**file-type** *content-obj-string2*]

Use the **no** form of this command to delete a file access control rule.

no file-rule *rule-id*

Parameter Description

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.
rule-id	Specifies the ID of a rule. The value ranges from **1** to **200** and a maximum of 200 rules are supported.
time-name	Specifies the time object name of a rule validity period.
comment-string	Specifies the rule description.
content-obj-string1	Specifies the file name keyword.
content-obj-string2	Specifies the file type keyword.

Defaults This command is not configured by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config**

command does not display the priority swap command.

Configuration Examples

1. #Delete all file rules from a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# file-rule delete-all
FS(cont-plcy-config)# end
```

2. #Swap priorities of file access control rules 10 and 20 in a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# file-rule priority-swap 10 20
FS(cont-plcy-config)# end
```

3. #Add a file access audit rule to a content audit policy group named policyA, to filter file names and audit the file names that are filtered out.

```
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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

1. If a configured rule ID already exists, the prompt is as follows:

```
FS(config)# file-rule 2 time-range any action deny audit comment TEST
Rule 2 already exists, please delete it first
```

Common Errors

N/A

Platform Description

This command is supported by products with built-in memories apart from the ACE series.

8.78 content-audit attach-to-elog enable

Use this command to enable the function of uploading information to the ELOG server as attachments.

content-audit attach-to-elog enable

Use the **no** form of this command to disable the function of uploading information to the ELOG server as attachments.

no content-audit attach-to-elog enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is valid in NPE mode.

Configuration Examples 1. #Enable the function of uploading information to the ELOG server in NPE mode.

```
FS# configure terminal
FS(config)# content-audit attach-to-elog enable
FS(config)# end
```

Verification Run the **show running-config** command to display the configuration status.

Prompt N/A

Common Errors N/A

Platform Description This command is supported by the EG2000XE/UE and EG3000XE/UE.

8.79 show report-function

Use this command to display whether reporting is enabled.

show report-function

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide

Configuration Examples

#Display whether reporting is enabled.

```
FS#show report-function
```

8.80 show report-custom-config

Use this command to display custom report configuration.

show report-custom-config { *rule-id* }

Parameter Description

Parameter	Description
rule-id	Specifies the report rule ID.

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Examples

#Display all custom report configuration.

```
FS#show report-custom-config
```

8.81 show report-custom-data

Use this command to display custom report data.

show report-custom-data *rule-id*

Parameter Description

Parameter	Description
rule-id	Specifies the report rule ID.

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Examples

#Display report data generated by custom report rule 1.

```
FS#show report-custom-data 1
```

8.82 url-rule

Use this command to enable the URL default audit function.

url-rule audit-default-enable

Use the **no** form of this command to disable the URL default audit function.

no url-rule audit-default-enable

Use this command to delete all URL rules in a policy group.

url-rule delete-all

Use this command to swap priorities of URL access control rules.

url-rule priority-swap *rule-id1 rule-id2*

Use this command to add a URL access control rule to a content audit policy group.

url-rule *rule-id* **url-object** *url-obj-name* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**comment** *comment-string*]

Use the **no** form of this command to delete a URL access control rule.

no url-rule *rule-id*

Use this command to enable the URL loose whitelist function.

url-rule apply-referer

Use the no form of this command to disable the URL loose whitelist function.

no url-rule apply-referer

Parameter Description

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.
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.

Defaults The URL rule function is disabled by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.
5. 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.
6. 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. This command is used to configure the URL whitelist policy. All the websites and their sub-sites in the whitelist are loosened.

Configuration Examples

1. #Enable the URL default audit function.

```
FS# configure terminal
FS(config)# content-policy _AUDIT_DEFAULT
FS(cont-plcy-config)# url-rule audit-default-enable
FS(cont-plcy-config)# end
```

2. #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
```

3. #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
```

4. #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
```

5. # Enable URL loose whitelist function.

```
FS# configure terminal
FS(config)#url-rule apply-referer
FS(config)#end
```

Verification Run the **show running-config** command to display the configuration status.

Prompt Information If the configured URL ID already exists, the following prompt information is displayed:

```
FS(config)# url-rule 2 url-object url-objA time-range any action deny audit
Rule 2 already exists, please delete it first
```

8.83 vid-rule

Use this command to enable virtual identity audit.

vid-rule audit-default-enable

Use the **no** form of this command to restore the default setting.

no vid-rule audit-default-enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Content audit policy group configuration mode

Default Level 14

Usage Guide The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable virtual identity audit.

```
FS# configure terminal
FS(config)# content-policy _AUDIT_DEFAULT
FS(cont-plcy-config)# vid-rule audit-default-enable
FS(cont-plcy-config)# end
```

Platform Description

This command is supported on products with built-in memory apart from the ACE series. And this command is also supported on the NBR-E and EG2000F series.

8.84 web-bbs-rule

Use this command to enable Web BBS audit.

web-bbs-rule audit-default-enable

Use this command to disable Web BBS audit.

no web-bbs-rule audit-default-enable

Use this command to delete all Web BBS rules in a policy group.

app-rule delete-all

Use this command to swap priorities of the Web BBS rules.

web-bbs-rule priority-swap *rule-id1 rule-id2*

Use this command to add a Web BBS rule to a content audit policy group.

web-bbs-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

Use the **no** form of this command to delete a Web BBS rule.

no web-bbs-rule *rule-id*

Parameter Description

Parameter	Description
rule-id1	The ID of rule 1 of which the priority is to be swapped.
rule-id2	The ID of rule 2 of which the priority is to be swapped.
rule-id	The ID of a rule. A value range is 1 to 200.
time-name	The name of a time object in a rule validity period.
content-object-name	The name of a content object.
comment-string	The description of a rule.

Defaults

Web BBS audit is disabled by default.

Command Mode

Content audit policy group configuration mode

Default Level

14

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. 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.
5. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable Web BBS audit.

```
FS# configure terminal
FS(config)# content-policy _AUDIT_DEFAULT
FS(cont-plcy-config)# web-bbs-rule audit-default-enable
FS(cont-plcy-config)# end
```

2. #Delete all Web BBS rules in a policy group.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# web-bbs-rule delete-all
FS(cont-plcy-config)# end
```

3. #Swap priorities of Telnet access control rules 10 and 20 in a policy group named 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
```

4. #Add a Web BBS audit rule to a content audit policy group named policyA, to filter Web BBS content.

```
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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

If the configured rule-id already exists, the prompt is as follows:

```
FS(config)# web-bbs-rule 2 time-range any content keyword-group action deny audit comment
```

```
DenyInvalidBBS

Rule 2 already exists, please delete it first
```

8.85 web-mail-rule

Use this command to enable Web mail audit.

web-mail-rule audit-default-enable

Use the **no** form of this command to disable Web mail audit.

no web-mail-rule audit-default-enable

Use this command to delete all Web mail rules in a policy group.

web-mail-rule delete-all

Use this command to swap priorities of Web mail rules.

web-mail-rule priority-swap *rule-id1 rule-id2*

Use this command to configure common part in a Web mail rule.

web-mail-rule *rule-id* **time-range** *time-name* [**direction** { **in** | **out** | **double** }] **action** { **permit** | **deny** } **audit** [**alarm**] [**comment** *comment-string*]

Use this command to add a Web mail rule to a content audit policy group.

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*]

Use this command to delete a Web audit rule.

no web-mail-rule *rule-id*

Parameter Description

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.
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-object-name1	Specifies a sender. If this parameter does not exist, it indicates that *content-object-name1* does not need to be matched.
content-object-name2	Specifies a receiver. If this parameter does not exist, it indicates that *content-object-name2* does not need to be matched.
content-object-name3	Specifies a mail subject. 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. 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. If this parameter does not exist, it indicates that *content-object-name5* does not need to be matched.

Defaults Web mail audit is disabled by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. When a rule is set to blocking, only the OR relation is valid.

5. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.

6. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable Web mail audit.

```
FS# configure terminal
FS(config)# content-policy _AUDIT_DEFAULT
FS(cont-plcy-config)# mail-rule audit-default-enable
FS(cont-plcy-config)# end
```

2. #Delete all Web 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
```

3. #Swap priorities of Web audit 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
```

4. #Add a Web audit 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
```

Verification

Run the **show running-config** command to display the configuration status.

Prompt

1. If the configured rule ID already exists, the prompt is as follows:

```
FS(config)# mail-rule 1 time-range any action permit audit comment mail-audit-1
Rule 1 already exists, please delete it first
```

2. If description of an Web mail rule is configured before the common part, the prompt is as follows:

```
FS(config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000
Rule 1 is not exist
```

8.86 web-search-rule

Use this command to enable Web search audit.

web-search-rule audit-default-enable

Use the **no** form of this command to disable Web search audit.

no web-search-rule audit-default-enable

Use this command to delete all Web search rules in a policy group.

web-search-rule delete-all

Use this command to swap priorities of Web search rules.

web-search-rule priority-swap *rule-id1 rule-id2*

Use this command to configure common part in a Web search rule.

web-search-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

Use this command to delete a Web search rule.

no web-search-rule *rule-id*

Parameter Description

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.
rule-id	Specifies the ID of a rule. The value ranges from 1 to 200 and a maximum of 200 rules are supported.
time-name	Specifies the time object name of a rule validity period.
content-object-name	Specifies the name of a content object used in a rule.
comment-string	Specifies the rule description.

Defaults Web search audit is disabled by default.

Command Mode Content audit policy group configuration mode

Default Level 14

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. This priority swap command is used to swap priorities of two access control rules. After this command is run, run the **show running-config** command to display a change in ranks of the two rules. Output of the **show running-config** command does not display the priority swap command.

5. The default audit function is valid only to a default audit policy group named **_AUDIT_DEFAULT**.

Configuration Examples

1. #Enable Web search audit.

```
FS# configure terminal
FS(config)# content-policy _AUDIT_DEFAULT
FS(cont-plcy-config)# web-search-rule audit-default-enable
FS(cont-plcy-config)# end
```

2. #Delete all Web search rules from a policy group named policyA.

```
FS# configure terminal
FS(config)# content-policy policyA
FS(cont-plcy-config)# web-search-rule delete-all
FS(cont-plcy-config)# end
```

3. #Swap priorities of Web search rule 10 and 20 in a policy group named 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
```

4. #Add a Web search rule to a content audit policy group named policyA, to filter out files that contain keywords in

keyword-group and audit the files that contain such keywords.

```
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
```

9 LINE-QUALITY Commands

9.1 debug line-quality track

Use this command to enable the line detection debugging switch. Use the **no** form of this command to disable the line detection debugging switch. Use the **default** form of this command to restore default settings.

debug line-quality track

no debug line-quality track

default debug line-quality ping

default debug line-quality track

Parameter Description

Parameter	Description
N/A	N/A

Defaults The line detection debugging switch is disabled by default.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Debugging information about the following events generated during module running is contained:

Track message processing event

CLI execution event

Other running exception events

Viewing debugging information of an abnormal event can help diagnose and locate faults.

Configuration Examples The following example enables the debugging switch for line quality monitoring.

```
FS# debug line-quality track
```

The following example disables the debugging switch for line quality monitoring.

```
FS# no debug line-quality track
```

Debugging Information 1. Track message processing event

Debugging Information	*Nov 1 17:43:36: %LQ-7-DEBUG: [lq_track_msg_proc:1079]recv track 300, state up.
Description	**track 300** indicates a track object whose ID is 300. **state** indicates the state of received information, including up, down, undefined, and obj_undef. A message is sent when a track is added or deleted, or an event is triggered.
Cause	A track is added or deleted, or an event is triggered.
Troubleshooting Suggestion	N/A

2. CLI execution event

Debugging Information	*Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:enable *Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:config *Nov 1 17:43:34: %LQ-7-DEBUG: [lq_cil_exec_result:26]CLI-R:Enter configuration commands, one per line. End with CNTL/Z. *Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:no track 300 *Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:no ip rns 300 *Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:ip rns 300 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:icmp-echo www.baidu.com out-interface GigabitEthernet 0/5 next-hop 172.21.3.1 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:deep *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:threshold 2000 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:timeout 2000 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:frequency 10000 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:exit *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:track 300 rns 300 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:delay up 60 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:delay down 60 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:exit
Description	This CLI execution event adds track and RNS configuration.
Cause	Line detection is configured, or the line status is changed.
Troubleshooting Suggestion	N/A

9.2 line-quality track enable

Use this command to enable line detection. Use the **no** form of this command to disable line detection.

line-quality track enable

no line-quality track enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Line detection is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Enabling or disabling line detection does not delete the configuration, and the configuration is still valid.

⚠ If a line is once disabled during line detection, the line will be enabled after the line detection function is disabled.

Configuration Examples

The following example enables line detection.

```
FS(config)# line-quality track enable
```

9.3 line-quality track set log-only

Use this command to record only the line detection result and not to enable or disable an interface. Use the **no** form of this command to disable recording only the line detection result.

line-quality track set log-only

no line-quality track set log-only

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Recording logs only is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Recording logs only is disabled by default. It is enabled only to view the line detection effect without disabling an interface. It is not recommended to be enabled for a long time.

⚠ As an interface is not enabled or disabled, the delivered track or RNS configuration is based on the original logic.

Configuration Examples

The following example enables recording logs only for line detection.

```
FS(config)# line-quanlity set log-only
```

9.4 line-quality track set flow-gate

Use this command to not disable an interface when the interface traffic reaches the threshold during line detection. Use the **no** form of this command to disable an interface when the interface traffic reaches the threshold.

line-quality track set flow-gate *percent*

no line-quality track set flow-gate

Parameter Description

Parameter	Description
percent	Percentage of traffic to the interface bandwidth

Defaults

50%

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to not disable an interface when the interface traffic reaches the threshold. This prevents packet loss and misjudgment due to heavy interface traffic.

Configuration Examples The following example sets the interface traffic threshold to 60%.

```
FS(config)# line-quanlity track set flow-gate 60
```

9.5 line-quality track set interface

Use this command to set the source IP address for monitoring line detection. Use the **no** form of this command to cancel the source IP address setting for monitoring line detection.

line-quality track set interface *interface-name* **source** *ipaddr*

no line-quality track set interface *interface-name* **source**

Parameter Description

Parameter	Description
interface-name	Interface name
ipaddr	Source IP address

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used in special scenarios to ensure normal detection, for example, public network mode or multiple WAN interfaces in the same network segment.

⚠ If this command is not configured in special scenarios, detection misjudgment may occur.

Configuration Examples The following example sets the source IP address for monitoring line detection.

```
FS(config)# line-quanlity track set interface g 0/5 source 172.21.3.55
```

Verification Run the **show line-quality track interface g 0/6** command to display the configured source IP address.

9.6 line-quality track set timeout

Use this command to set the line detection timeout time. Use the **no** form of this command to cancel the configured line detection timeout time.

line-quality track set timeout *msecs*

no line-quality track set timeout

Parameter Description

Parameter	Description
msecs	Line detection timeout time, in milliseconds

Defaults

2000 ms

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Generally, the default timeout time is used. If a higher detection precision is required, set the timeout time to a smaller value.

Configuration Examples

The following example enables line quality monitoring.

```
FS(config)# line-quanlity track set timeout 1000
```

Verification

Run the **show line-quality track** command to display the value of **line quality track timeout**.

9.7 line-quality track set { up | down }

Use this command to set the line detection frequency and acknowledgment time. Use the **no** form of this command to cancel the configured line detection frequency and acknowledgment time.

line-quality track set { up | down } frequency *f-secs* **delay** *d-secs*

no line-quality track set { up | down }

Parameter Description

Parameter	Description
f-secs	Line detection frequency, in seconds
d-secs	Line detection acknowledgment time, in seconds

Defaults

When an interface is up, the detection frequency is 10s and the acknowledgment time is 12s.

When an interface is down, the detection frequency is 3s and the acknowledgment time is 60s.

Command Mode

Global configuration mode

Default Level

14

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. Otherwise, the detection status and policy frequently change, which may affect network stability. In addition, the acknowledgment time for enabling a disabled interface must be long enough (60s by default). Otherwise, an unstable network may be misjudged as good, resulting in frequent up and down of the interface.

Configuration Examples

The following example sets the delay to disable a line to 300s.

```
FS(config)# line-quanlity set down frequency 3 delay 300
```

Verification

Run the **show line-quality track** command. In the command output, the following two lines display the configured detection frequency and acknowledgment time:

```
line quality track up      :[freq:10 ; delay:12 ]
line quality track down  :[freq:3 ; delay:60 ]
```

9.8 line-quality track permit-interface

Use this command to configure an interface that can be detected. Use the **no** form of this command to disable line detection for the interface.

line-quality track permit-interface *interface-name*

no line-quality track permit-interface *interface-name*

Parameter Description

Parameter	**Description**
interface-name	Interface name

Defaults

The line detection switch displayed on the web page for an interface is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Generally, the primary line is set as the configurable line. This configuration is not mandatory and only used as a basis for interface selection on the web page.

⚠ If this command is not configured, a web application cannot select this interface during configuration.

Configuration Examples

The following example sets the G0/5 interface to be detectable.

```
FS(config)# line-quanlity track permit-interface g 0/5
```

Verification Run the **show line-quality track** command. The following fields are displayed:

line quality permit interface:

[5] GigabitEthernet 0/6

9.9 line-quality track interface interface-name enable

Use this command to enable detection for a line. Use the **no** form of this command to disable detection for a line.

line-quality track interface *interface-name* **enable**

no line-quality track interface *interface-name* **enable**

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults Detection is disabled for a line by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide To configure interface detection information, enable detection for the interface first. If detection is disabled for the interface, existing configurations of the interface will be cleared.

⚠ If the protocol status of the interface is down before the detection function is disabled, the protocol status will first change to up.

Configuration Examples The following example enables line quality monitoring.

```
FS(config)# line-quanlity track interface g 0/5 enable
```

Verification Run the **show line-quality track interface g 0/5** command.

The command output displays GigabitEthernet 0/5, index:4, stat:USED, ctrl:UP, source 0.0.0.0.

The **stat** value of **USED** or **STOP** indicates that the function is enabled. If the function is disabled, **stat** is not displayed or is **DEL**.

9.10 line-quality track interface interface-name { icmp | dns | tcp }

Use this command to configure ICMP line detection. Use the **no** form of this command to cancel ICMP line detection.

line-quanlity track interface *interface-name* **icmp { enable |** *ip* **|** *url* **}**

no line-quanlity track interface *interface-name* **icmp [enable]**

Use this command to configure DNS line detection. Use the **no** form of this command to cancel DNS line detection.

line-quality track interface *interface-name* **dns { enable |** *ip* **}**

no line-quanlity track interface *interface-name* **dns [enable]**

Use this command to configure TCP line detection. Use the **no** form of this command to cancel TCP line detection.

line-quality track interface *interface-name* **tcp { enable |** *ip* **|** *url* **}**

no line-quanlity track interface *interface-name* **tcp [enable]**

Parameter Description

Parameter	Description
interface-name	Interface name
enable	Enable line detection of a protocol. When line detection of a protocol is disabled, the protocol configuration is not cleared.
ip	IP address of the detection objective
url	URL of the detection objective

Defaults Line detection is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide To enable detection for an interface, generally, you need to first configure the detection objective and then enable the protocol.

The detection objective can be an IP address or a URL. If both the IP address and URL are configured, the IP address is preferentially selected as the detection objective.

If multiple detection protocols are enabled, comply with the following rules:

- If ICMP line detection is enabled and succeeds, do not perform DNS or TCP line detection.
- If ICMP line detection is not enabled or fails, perform DNS and TCP line detection.
- An interface is regarded as normal if any of the ICMP, DNS, and TCP line detections succeeds.
- An interface is regarded as abnormal if all the ICMP, DNS, and TCP line detections fail.
- If no detection objective is configured for ICMP line detection, the next-hop is detected by default. If no detection objective is configured for DNS or TCP line detection, detection is not performed.

⚠ Configuring multiple protocols can increase the detection accuracy. However, it also prolongs judgment and consumes more resources.

Configuration Examples The following example configures ICMP line detection on the G0/5 interface to check whether www.baidu.com is reachable.

```
FS(config)# line-quanlity track interface g 0/5 icmp www.baidu.com
FS(config)# line-quality track interface g 0/5 icmp enable
```

Verification Run the **show line-quality track interface g 0/5** command. The command output is as follows, and the red part is the configured content.

```
GigabitEthernet 0/5, index:4, stat:USED, ctrl:UP, source 0.0.0.0
  ICMP: enable
    url: www.baidu.com
    ip : 0.0.0.0
```

```
     track_id : 300; rns_id: 300
     track_msg: UP; track_stat: UP
     last time: 2016-11-02 12:03:28
   DNS: disable
     ip : 0.0.0.0
     track_id : 0; rns_id: 0
     track_msg: NONE; track_stat: NONE
     last time:
   TCP: disable
     url:
     ip : 0.0.0.0
     track_id : 0; rns_id: 0
     track_msg: NONE; track_stat: NONE
     last time:
```

9.11 line-quality track interface interface-name up

Use the command to enable an interface at the protocol layer. Use the **no** form of this command to disable an interface at the protocol layer.

line-quality track interface *interface-name* **up**

no line-quality track interface *interface-name* **up**

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

When the detection result is incorrect, you can manually enable or disable an interface.

⚠ This configuration takes effect only at the protocol layer.

Configuration Examples

The following example enables the G0/5 interface at the protocol layer.

```
FS(config)# line-quanlity track interface g 0/5 up
```

Verification

Run the **FS#show line-quality track interface line** command.

```
Interface                    Status Protocol Last-ctrl
GigabitEthernet 0/5         UP       UP          --
GigabitEthernet 0/6         UP       UP          --
```

9.12 show line-quality track

Use this command to display line detection configuration.

show line-quality track

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

This command is used to display interface detection parameter configuration on a device.

Configuration Examples

The following example displays detection information of all line quality monitoring interfaces.

```
FS#show line-quality track
line quality track                :enable
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:3    ; delay:60 ]
line quality permit interface:
   [5] GigabitEthernet 0/6
```

Field description:

Field	Description
line quality track	Interface detection switch
line quality track log-only	Indicates whether only logs are recorded.
line quality track flow-gate	Traffic threshold. When the interface traffic reaches the percentage to the bandwidth, the interface is not disabled.
line quality track timeout	Interface detection timeout time
line quality track intf count	Number of configured interfaces
line quality track up/down	Detection frequency and acknowledgment time in interface up and down states
line quality permit interface	List of interfaces that allow detection

9.13 show line-quality track interface

Use this command to display the information and status of the detection function configured at an interface.

show line-quality track interface [*interface-name*]

Parameter

Parameter	Description

Description

interface-name	Specifies the interface to query. If no interface is specified, all interfaces are queried.

Command Mode

Privileged EXEC mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

This command is used to display line detection information and status of an interface.

Configuration Examples

The following example displays line detection information and status of an interface.

```
FS#show line-quality track interface g 0/5
GigabitEthernet 0/5, index:4, stat:USED, ctrl:UP, source 0.0.0.0
  ICMP: enable
    url: www.baidu.com
    ip : 0.0.0.0
    track_id : 300; rns_id: 300
    track_msg: UP; track_stat: UP
    last time: 2016-11-02 16:34:19
  DNS: disable
    ip : 0.0.0.0
    track_id : 0; rns_id: 0
    track_msg: NONE; track_stat: NONE
    last time:
  TCP: disable
    url:
    ip : 0.0.0.0
    track_id : 0; rns_id: 0
    track_msg: NONE; track_stat: NONE
    last time:
```

Field description:

Field	Description
index	Interface index
stat	Status of the line detection function configured at an interface. **USED** indicates that the function is being used, **STOP** indicates that the function is paused, and **DEL** indicates that the function is deleted.
ctrl	Interface control status. **UP** indicates that the interface is enabled, **DOWN** indicates that the interface is disabled, and **NONE** indicates that the interface is not controlled.
source	Source IP address of the interface
ICMP/DNS/TCP	Detection protocol switch. **enable** indicates that the protocol is enabled, and **disable** indicates that the protocol is disabled.
url/ip	Detection objective address

track_id,rns_id	Track and RNS IDs corresponding to detection
track_msg	Last detection message type
track_stat	Current detection status
last time	Last detection message reach time

9.14 show line-quality track interface line

Use this command to display the line status.

show line-quality track interface line

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

This command is used to display the physical status and protocol status of all interfaces that allow detection, and the last control status of line detection.

Configuration Examples

The following example displays the status information of an interface, including the physical status and protocol status at the link layer.

```
FS#show line-quality track interface l
Interface                         Status Protocol Last-ctrl
GigabitEthernet 0/5              UP      UP       UP
GigabitEthernet 0/6              UP      UP       --
```

Field description:

Field	**Description**
Interface	Interface name
Status	Physical status of an interface
Protocol	Protocol status of an interface
Last-ctrl	Last control status of line detection

9.15 show line-quality log

Use this command to display module logs.

show line-quality log [**type** *type-num*] [**limit** *count*]

Parameter Description

Parameter	**Description**
type *type-num*	Log type
limit *count*	Limited log quantity

Command Mode

Privileged EXEC mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

This command is used to display log information of LINE-QUALITY.

Configuration Examples

The following example displays log information of LINE-QUALITY.

```
FS#show line-quality log limit 5
time                          type log
------------------------------
2016-11-02 16:34:42 2       interface 4 track modify.
2016-11-02 16:34:42 22      interface 4 delay up, prot=ICMP.
2016-11-02 16:34:19 2       interface 4 track modify.
2016-11-02 16:34:19 22      recv track 300 event, state=up.
2016-11-02 16:34:16 4       interface 4 add track 300, prot=ICMP, state=UP.
```

Field description:

Field	Description
time	Log time
type	Log type
log	Log message

Chapter 4 Device Management Commands

1 Device Audit Commands

1.1 dev-audit enable

Use this command to enable the device audit function.

dev-audit enable

Use the **no** form of this command to disable the device audit function.

no dev-audit enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The device audit function is enabled by default.

Command Mode Global configuration mode

Default Level 15

Usage Guide Data about device audit is recorded in the local database of devices.

⚠ If the recorded data is not stored locally, only logs are sent. The data cannot be displayed locally.

Configuration Examples #Enable the device audit function.

```
FS(config)# dev-audit enable
```

Verification Run the **show run** command to check whether the device audit function is enabled.

1.2 show dev-audit

Use this command to display device audit record.

show dev-audit {**cpu** | **memory** | **flash**} **from** *year* [*month* [*mday* [*hh:mm:ss*]]] [**to** *year* [*month* [*mday* [*hh:mm:ss*]]]]

Parameter Description

Parameter	Description
cpu	CPU usage
memory	Memory usage
flash	Flash record, including the usage of flash, SATA hard disk, or USB flash drive
from *year* [*month* [*mday* [*hh:mm:ss*]]]	Specifies the time of displayed information, namely, the start time.
to *year* [*month* [*mday* [*hh:mm:ss*]]]	Specifies the time of displayed information, namely, the end time.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 15

Usage Guide This command is used to display device audit record.

Configuration Examples

#Display CPU record.

```
FS#show dev-audit cpu from 2013 9 2
Date & Time                CPU
2013-09-02 12:03:11        2%
2013-09-02 12:08:11        2%
2013-09-02 12:13:11        3%
2013-09-02 12:18:11        2%
2013-09-02 12:23:11        2%
2013-09-02 12:28:11        2%
```

Field description: Field	Description
Date & Time	Record time
CPU	CPU usage

#Display flash record.

```
FS#show dev-audit flash from 2013 9 2 12:00:00
Date & Time             Flash-Total(KB)         Flash-Free (KB)      SATA-Total(MB) SATA-Free(MB)

2013-09-02 12:12:11             523776       454592       143372       140859
2013-09-02 13:11:11             523776       454592       143372       140858
2013-09-02 14:10:11             523776       454592       143372       140858
2013-09-02 15:09:11             523776       454592       143372       140857
```

Field description: Field	Description
Date & Time	Record time
CPU	CPU usage
Flash-Total (KB)	Total space of flash
Flash-Free (KB)	Hard disk data in the available space of flash
SATA-Total(MB)	Total space of SATA hard disk
SATA-Free(MB)	Available space of SATA hard disk
USB-Total(MB)	Total space of USB flash drive
USB-Free(MB)	Available space of USB flash drive
Avail-Buff	Number of available buffers
v4-Flow	Number of current IPv4 flows
Input-Rate	Interface receiving rate
Output-Rate	Interface transmission rate
No-Buffer	Number of **no buffer** alarms on an interface

Prompt Information

The following error message is displayed if data is not stored in the local database of devices:

```
Data is not stored in the local !
```

2 USB Commands

2.1 show usb

Use this command to display the information about the inserted USB device in the system.

show usb

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Device information is displayed if there is a USB device. Otherwise, there is no output. If the USB disk is connected to the USB port on the device, the ID displayed by running the **show usb** command is X, the USB port number. If the USB disk is connected to the USB port on the device via a HUB, the ID displayed by running the **show usb** command is X-Y, in which X stands for the USB port number and Y for the HUB slot number.

Configuration Examples

The following example displays the information about the USB device:

```
FS# show usb
Device: Mass Storage:
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:FAT32)
Size : 131,072,000B(125MB)
Available size: 1,260,020B(1.2MB)
```

In above information, the Mass Storage Device is the name of the device.

The meaning of the information is as below:

Table 1: the description of the field.

Field	Description
URL	Prefix used to access the USB device.
Size	Accessible size of the USB device.
Available size	Available size of the USB device.

Related Commands

Command	Description

N/A	N/A

Platform Description

N/A

2.2 usb remove

Use this command to remove the USB device.

usb remove *device_id*

Parameter Description

Parameter	Description
device_id	Device ID of USB to be removed.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Before pulling out the USB device, you need to remove the device using a command, so as to prevent errors that may occur because the system is using the device. If the device is removed successfully, the system will show a prompt, when you can pull out the device. If the device cannot be pulled out, it indicates that the system is using this USB device, so you have to wait a moment before removing it again.

Configuration Examples

The following example removes the USB device.

```
FS# usb remove 0
OK, now you can pull out the device 0.
```

At this moment, the USB device can be plugged out.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3 SYS Commands

3.1 calendar set

Use this command to set the hardware calendar.

calendar set { *hour* [*:minute* [*:second*]] } [*month* [*day* [*year*]]]

Parameter Description

Parameter	Description
hour [:minute [:second]]	Sets hardware time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can be reset. The unspecified parameters keep the current system values.
month	Sets month. The range is from 1 to 12.
day	Sets date. The range is from 1 to 31. If the day does not exist in the current month, the date is calculated backward.
year	Sets year. The range is from 1970 to 2069.

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide

1. The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value. For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the **calendar set** *12 5* command to change the current time into "2012-05-29 12:33:44".
2. If the value of parameter *day* is between 1 and 31, but the current month does not contain that day, the value will be calculated backward. For example, February 2012 has 29 days. If you use the **calendar set** *11:30 2 31 2012* command to set the date to February 31, by default, the system adds two days backwards. Therefore, the current hardware time is "2012-03-02 11:30:23".

ⓘ The hardware time of the system is used as the UTC time, while the software time of the system refers to the local time of the device.

ⓘ This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 6 o’clock and keeps the values of other parameters.

```
FS# calendar set 6
06:41:39 UTC Fri, Jul 6, 2012
```

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters.

```
FS# calendar set 6:42
06:42:27 UTC Fri, Jul 6, 2012
```

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.

```
FS# calendar set 18 3 2
18:43:05 UTC Fri, Mar 2, 2012
```

⚠ Because the *hour* parameter is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter **18** (hour), and then enter **3** (month) and **2** (day).

Check Method -

Platform Description -

3.2 clock read-calendar

Use this command to enable the system to synchronize the software time with the hardware time.

clock read-calendar

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

After you configure this command, the system will synchronize the software time with the current hardware time according to the time zone and summer time settings of the device.

Configuration Examples The following example enables the system to synchronize the software time with the hardware time.

```
FS# clock read-calendar
Set the system clock from the hardware time.
```

Check Method -

Platform Description -

3.3 clock set

Use this command to set the system software clock.

clock set { *hour* [*:minute* [*:second*]] } [*month* [*day* [*year*]]]

Parameter Description

Parameter	Description
hour [:minute [:second]]	Sets software time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can reset. The unspecified parameters keep the current system values.
month	Sets month. The range is from 1 to 12.
day	Sets date. The range is from 1 to 31. If the day does not exist in the current month, the date is calculated backward.
year	Sets year. The range is from 1970 to 2069.

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide

1. The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value.

For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the **clock set** *12 5* command to change the current time into "2012-05-29 12:33:44".

2. If the value of parameter *day* is between 1 and 31, but the current month does not contain that day, the value will be calculated backward.

For example, February 2012 has 29 days. If you use the **clock set** *11:30* 2 31 2012 command to set the date to February 31, by default, the system adds two days backward. Therefore, the current hardware time is "2012-03-02 11:30:23".

This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 6 o’clock and keeps the values of other parameters.

```
FS# clock set 6
06:48:13 CST Fri, Mar 2, 2012
```

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters.

```
FS# clock set 6:42
06:42:31 CST Fri, Mar 2, 2012
```

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.

```
FS# clock set 18 3 2
18:42:48 CST Fri, Mar 2, 2012
```

⚠ Because the *hour* parameter in this command is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter **18** (hour), and then enter **3** (month)
and **2** (day).

Check Method -

Platform Description -

3.4 clock summer-time

Use this command to set the summer time.

clock summer-time *zone* **start** *start-month* [*week*|**last**] *start-date hh:mm* **end** *end-month* [*week*| **last**] *end-date hh:mm* [**ahead** *hours-offset* [*minutes-offset*]

Use this command to disable the summer time.

no clock summer-time

Parameter Description

Parameter	**Description**
zone	Summer time name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The summer time name contains 3 to 31 characters.
start	Indicates the start time of the summer time.
start-month	Start month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Febr and FebRu.
week	Start week in the start month. The range is from 1 to 5.
last	The last week of the specified month.
start-date	Day in the start week of the start month. Value range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Web and WeDne.
hh:mm	Time, in the format of hour : minute.
end	Indicates the end time of the summer time.
end-month	End month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you may enter an incomplete word, for example, Febr and FebRu.
ahead	Indicates how much time for the summer time ahead of the standard time during the effective period of the summer time. By default, the summer time is one hour ahead of the standard time.
hours-offset	Hours ahead of the standard time. The range is from 0 to 12. You are not allowed to set it to 00:00.
minutes-offset	Minutes ahead of the standard time. The range is from 0 to 59. If *hours-offset* has been set to 0, you are not allowed to set *minutes-offset* to 0.

Defaults -

Command Mode Global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples

Assume that the time zone name of your living place is ABC and the standard time is 8:15 ahead of UTC, namely, GMT+08:15. The summer time period starts from the first Saturday in February to the third Monday in May and the summer time is 01:20 ahead of the standard time. In this case, the summer time is 09:35 ahead of the UTC time, but non-summer time is still 08:15 ahead of the UTC time.

```
FS(config)# clock timezone ABC 8 15
Set time zone name: ABC (GMT+08:15)
FS(config)#show clock
16:39:16 ABC Wed, Feb 29, 2012
FS(config)#show calendar
```

```
08:24:35 GMT Wed, Feb 29, 2012

FS(config)# clock summer-time TZA start Feb 1 sat 2:00 end May 3 Monday 18:30 ahead 1 20
*May 10 03:45:58: %SYS-5-CLOCKUPDATE: Set summer-time: TZA from February the 1st Saturday at 2:00 TO May
the 3rd Monday at 18:30, ahead 1 hour 20 minute
Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at 18:30, ahead 1 hour 20
minute

FS# show clock
18:00:08 TZA Wed, Feb 29, 2012

# If the time is set to non-summer time, the time zone name is restored to ABC.
FS#clo set 18 1 1
*Jan  1 18:00:09: %SYS-5-CLOCKUPDATE: Set system clock: 18:00:09 ABC Sun, Jan  1, 2012
Set system clock: 18:00:09 ABC Sun, Jan  1, 2012
FS#show clock
18:00:12 ABC Sun, Jan  1, 2012
```

If the system uses the default summer time that is one hour ahead of the standard time, ahead and the parameters behind ahead can be neglected. For example, set the summer time to start from 2:00 a.m. of the first Sunday in April to 2:00 a.m. of the last Sunday in October and set the summer time to one hour ahead of the standard time.

```
FS(config)#clo summer-time PDT start April 1 sunday 2:00 end October last Sunday 2:00
*May 10 03:15:05: %SYS-5-CLOCKUPDATE: Set summer-time: PDT from April the 1st Sunday at 2:00 TO October
the last Sunday at 2:00, ahead 1 hour
Set summer-time: PDT from April the 1st Sunday at 2:00 TO October the last Sunday at 2:00, ahead 1 hour
```

The following example disables summer time.

```
FS(config)#no clock summer-time
*Jan  1 18:01:09: %SYS-5-CLOCKUPDATE: Set no summer time.
Set no summer time.
```

Check Method -

Platform Description -

3.5 clock timezone

Use this command to set the time zone.

clock timezone [*name hours-offset* [*minutes-offset*]]

Use this command to remove the time zone settings.

no clock timezone

Parameter

Parameter	Description

Description

name	Time zone name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The name contains 3 to 31 characters.
hours-offset	Hours of time difference. It indicates whether the time is faster or smaller than the hardware UTC time. The range is from -12 to 12. The negative digit indicates that the time is slower than the hardware time, while the positive digit indicates that the time is faster than the hardware time. ℹ If the time is slower than the UTC time, add "-" before *hours-offset*.
minutes-offset	Minutes of time difference. The range is from 0 to 59.

Defaults -

Command Mode Global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples

The following example sets the time zone name to CST. The software time is 8 hours faster than the hardware time.

```
FS(config)# clock timezone CST 8
Set time zone name: CST (GMT+08:00)

FS# show clock
18:00:17 CST Wed, Dec 5, 2012
```

The following example sets the time zone name TZA. The software time is 06:13 slower than the hardware time.

```
FS(config)# clock timezone TZA -6 13
Set time zone name: TZA (GMT-06:13)
```

The following example removes the time zone settings.

```
FS(config)# no clock timezone
Set no clock timezone.
```

Check Method -

Platform Description -

3.6 clock update-calendar

Use this command to enable the system to synchronize the hardware time with the software time.

clock update-calendar

Parameter Description

Parameter	Description
-	-

Defaults -

Command Mode Privileged EXEC mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

After you configure this command, the system will synchronize the hardware time with the current software time according to the time zone and summer time settings of the device.

Configuration Examples The following example enables the system to synchronize the hardware time with the software time.

```
FS# clock update-calendar
Set the hardware time from the system clock.
```

The following example sets the time zone of the hardware time to GMT+5:10, which indicates that the hardware time is 5:10 slower than the software time. The summer time is not set.

```
FS# show clock
09:30:21 TSZ Wed, Feb 29, 2012

FS# clock update-calendar
Set the hardware time from the system clock.

FS#show calendar
04:20:25 UTC Wed, Feb 29, 2012
```

The following example sets the hardware time. If it is set to GMT+5:10 and the summer time is set to be 1:15 faster from the first Monday in February 1 to the second Sunday in June 1, it indicates that the hardware time is 6:25 slower than the software time during the effective period of the summer time.

```
FS# show clock
09:30:02 TSZ Wed, Feb 29, 2012

FS# clock update-calendar
Set the hardware time from the system clock.

FS#show calendar
03:05:08 UTC Wed, Feb 29, 2012
```

Check Method -

Platform Description -

3.7 cpu high-watermark set

Use this command to set the high watermark of the CPU usage of the control core and enable CPU usage monitoring.

cpu high-watermark set [[**high** *high-value*] [**range** *range-value*]]

Use this command to disable CPU usage monitoring.

no cpu high-watermark set

Use this command to restore the default settings.

default cpu high-watermark set

Parameter Description

Parameter	Description
high *high-value*	Sets the high watermark of the CPU usage. The range is from 2 to 99.
range *range-value*	Sets the watermark fluctuation range. The range is from 1 to 20.

Defaults

By default, the watermark of the CPU usage is 80% and the watermark fluctuation range is 5% (namely, the range of the CPU usage watermark is from 75% and 85%).

Command Mode

Global configuration mode

Default Level

-

Usage Guide

This command is supported only in VSD0 mode. Multiple VSDs are not supported.

You can use this command to set the high watermark of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the fluctuation range of the highest watermark, the system prints prompts.

Configuration Examples

The following example sets the CPU usage watermark to the default value and enables CPU usage monitoring (if it is disabled).

```
FS(config)# default cpu high-watermark set
Reset default cpu watermark monitor
set system cpu watermark high 80%(75%~85%)
```

The following example disables CPU usage monitoring.

```
FS(config)# no cpu high-watermark set
Close cpu watermark monitor
```

The following example enables CPU usage monitoring. Keep the defined watermark value.

```
FS(config)# cpu high-watermark set
Open cpu watermark monitor
set system cpu watermark high 80%(75%~85%)
```

The following example enables CPU usage monitoring and sets the high watermark to 88% and fluctuation range to 3%.

```
FS(config)# cpu high-watermark set high 88 range 3
Open cpu watermark monitor
set system cpu watermark high 88%(85%~91%)
```

In this case, the high watermark is set to 88%. The upper limit of the high watermark is 91% (88%+3%) and the lower limit is 85% (88%-3%).

Check Method

-

Prompt Message

If the high watermark of the CPU usage is allowed to fluctuate from 85% to 91%, the system will print the following warning message when the CPU usage exceeds the upper limit of the high watermark:

```
*Jan 19 16:23:01: %FS_SYSMON-4-CPU_WATERMARK_HIGH: warning! system cpu usage above high watermark(85%),current cpu usage 100%
```

When the CPU usage is less than the lower limit of the high watermark, the system will print the following message about warning release:

```
*Jan 20 07:02:52:    %FS_SYSMON-5- CPU_WATERMARK:withdraw warning! system cpu usage below high watermark(85%), current cpu usage 36%
```

Platform Description

-

3.8 memory history clear

Use this command to clear the history of the memory usage.

memory history clear [**one-forth** | **half** | **all**]

Parameter Description

Parameter	Description
one-forth	Clears one fourth entries.
half	Clears a half of entries.
all	Clears all the entries.

Defaults

-

Command Mode

Global configuration mode

Default Level

-

Usage Guide

-

Configuration Examples

The following example clears a half of the history of the memory usage.

```
FS# show memory history

Time Thu Jan   1 00:24:45 1970
Used(k) 148516
Maxinum memory users for this period
Process Name       Holding
tcpip.elf          270028
cli-memory          60600
rg_syslogd          36640

Time Thu Jan   1 00:24:41 1970
Used(k) 148492
Maxinum memory users for this period
Process Name       Holding
tcpip.elf          270028
cli-memory          52408
```

```
fs_syslogd          36640

Time Thu Jan    1 00:24:41 1970
Used(k) 148444
Maxinum memory users for this period
Process Name        Holding
tcpip.elf           270028
cli-memory          44088
fs_syslogd          36640

FS(config)#memory history clear half
2 out of 5 records in the history table to be cleared...
Clear done !
```

Check Method -

Prompt Message -

Platform Description -

3.9 memory low-watermark set

Use this command to set the low watermark threshold of the memory and enable the memory low watermark detection.

memory low-watermark set *mem-value*

Use this command to disable the detection of memory low watermark.

no memory low-watermark set

Parameter Description

Parameter	Description
mem-value	Memory watermark threshold. The range is from 1 KB to 4,294,967,295 KB.

Defaults By default, the detection of memory low watermark is disabled.

Command Mode Global configuration mode

Default Level -

Usage Guide You can use this command to enable the detection of the memory low watermark and set the memory watermark threshold. When the system memory is less than this threshold, the system will print prompts.

Configuration The following example sets the low watermark threshold of the memory to 500,000 KB and enables detection.

Examples

```
FS(config)#memory low-watermark 500000
```

Check Method

-

Prompt Message

When the system memory is less than the defined watermark value (such as 500000 KB), the system prints the following message:

```
FS(config)#<187> Jan    1 00:18:59 syslog: Free Memory has dropped below 500000k
```

Platform Description

-

3.10 reload

Use this command to reload the device.

reload [**at** { *hour* [*:minute* [*:second*]] } [*month* [*day* [*year*]]]

Parameter Description

Parameter	Description
hour [*:minute* [*:second*]]	Sets the restart time in the format of hour : minute : second. Other neglected parameters keep the current system values.
month	Sets the month, in the range from 1 to 12.
day	Sets the day, in the range from 1 to 31.
year	Sets the year, in the range from 1970 to 2069.

Defaults

-

Command Mode

Privileged EXEC mode

Default Level

-

Usage Guide

-

Configuration Examples

The following example reloads the device.

```
FS# reload
Reload system?(Y/N) Y
Sending all processes the TERM signal...                                   [    OK    ]
Sending all processes the KILL signal...                                  [    OK    ]
Restarting system...
```

Check Method

-

Prompt Message

-

Platform Description

-

3.11 show calendar

Use this command to display the hardware calendar.

show calendar

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Configuration Examples

The following example displays the hardware calendar.

```
FS# show calendar
21:57:48 GMT Sun, Feb 28, 2012
```

Prompt Message -

Platform Description -

3.12 show clock

Use this command to display the system software clock.

show clock

Parameter Description

Parameter	Description
-	-

Command Mode Privileged EXEC mode / global configuration mode

Default Level -

Usage Guide -

Configuration Examples

The following example displays the software clock when the time zone is disabled.

```
FS# show clock
18:22:20 UTC Tue, Dec 11, 2012
```

The following example displays the software clock when the time zone is enabled.

```
FS# show clock
```

```
03:07:49 TSZ Wed, Feb 29, 2012
```

Prompt Message -

Platform Description -

3.13 show cpu

Use this command to display the information on the system task running on the control core instead of the non-virtual core.

show cpu

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

If the system is equipped with a virtual core, you can use the **show processes cpu** command to check the CPU usage of the virtual core.

Configuration Examples The following example displays the information on the system task running on the control core instead of the non-virtual core.

```
FS#show cpu
================================================
CPU Using Rate Information
CPU utilization in five seconds:    4.80%
CPU utilization in one minute:    4.10%
CPU utilization in five minutes:    4.00%

 NO          5Sec       1Min        5Min Process
      1     0.00%      0.00%      0.00% init
      2     0.00%      0.00%      0.00% kthreadd
      3     0.00%      0.00%      0.00% ksoftirqd/0
      4     0.00%      0.00%      0.00% events/0
--More--
```

Prompt Message -

Platform -

Description

3.14 show memory

Use this command to display the system memory.

show memory [**sorted total** | **history** | **low-watermark** | *process-id* | *process-name*]

Parameter Description

Parameter	Description
sorted total	Ranked according to the memory usage.
history	Displays the history of memory usage.
low-watermark	Displays the memory low watermark threshold of the system.
process-id	Displays the memory usage of the task specified by *process-id*.
process-name	Displays the memory usage of the task specified by *process-name*.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide Every time when the **show memory history** command is used, the number of displayed entries increases by one. Up to 10 entries can be displayed. You can use the **memory history clear** command to clear history entries.

Configuration Examples The following example displays the memory usage of each task and the ranking (based on the total memory usage).

```
FS# show memory sorted
System Memory: 508324K total, 481560K used, 26764K free, 31.5% used rate
Used detail:     149112K active, 247776K inactive, 30460K mapped, 50460K slab, 3752K others

PID      Text(K) Rss(K)    Data(K)          Stack(K) Total(K)          Process
807      1568      4584      264728              84         270028             tcpip.elf
854      40        1436      246076              84         248840             cli-filesystem
1237     52        1492      123260              84         126036             cli-memory
803      56        1104      74064               84         76920              ping.elf
727      84        1276      33812               84         36640              fs_syslogd
733      84        796       33536               84         36364              fs_syslogd
776      224       1416      16896               84         19800              lsmdemo
858      40        1324      16844               84         19612              fs-tty-admin
769      40        3600      11052               84         13812              skbdemo
--More--
```

Description of some keywords in the command:

Keyword	Description
total	Total system memory
used	Used memory

free	Remaining memory
used rate	Memory usage (percentage)
Active	Active page
inactive	Inactive page
mapped	Mapped memory
slab	Memory consumed by Slab
others	Memory capacity of the used memory except the memory used by active and inactive pages, mapped memory, and slab memory.

Description of the displayed information on each task:

Field	Description
PID	Process ID
Text	Code segment size
Rss	Resident memory size
Data	Data segment size
Stack	Stack size
Total	Total used memory
Process	Task name

Prompt Message -

Platform Description -

3.15 show pci-bus

Use this command to display the information on the device mounted to the PCI bus.

show pci-bus

Parameter Description

Parameter	**Description**
-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Configuration Examples

The following example displays the information on the device mounted to the PCI bus.

```
FS# show pci-bus
NO:0
Vendor ID                : 0x1131
```

```
Device ID                    : 0x1561
Domain:bus:dev.func      : 0000:00:05.0
Status / Command            : 0x2100000
Class / Revision           : 0xc031030
Latency                          : 0x0
first 64 bytes of configuration address space:
00: 31 11 61 15 00 00 10 02 30 10 03 0c 20 00 80 00
10: 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 61 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 01 2a

NO:1
Vendor ID                     : 0x1131
Device ID                    : 0x1562
Domain:bus:dev.func      : 0000:00:05.1
Status / Command            : 0x2100156
Class / Revision           : 0xc032030
Latency                          : 0x30
First 64 bytes of configuration address space:
00: 31 11 62 15 56 01 10 02 30 20 03 0c 20 30 80 00
10: 00 10 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 62 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 02 10
```

Prompt Message -

Platform Description -

3.16 show processes cpu

Use this command to display system task information.

show processes cpu [**history** [**table**] | [**5sec | 1min | 5min | 15min**] [**nonzero**]]

Parameter Description

Parameter	Description
5sec | 1min | 5min | 15min	Displays lists of tasks in descending order of CPU usage within the last five seconds, one minute, five minutes, and 15 minutes.
Nonzero	Does not display the task with 0 CPU usage.
History	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in histogram.
Table	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in table.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples

The following example displays the tasks listed in ascending order of task IDs.

```
FS# show processes cpu
System Uptime: 19:08.6
CPU utilization for five seconds:1.2%; one minute:0.8%; five minutes:0.8%
set system cpu watermark (open): high 80%(85%~75%)

Tasks Statistics: 375 total, 10 running, 365 sleeping, 0 stopped, 0 zombie
  Pid Vsd S    PRI   P         5Sec          1Min          5Min        15Min Process
    1    0 S     20   0    0.0(0.0)     0.0(0.0)     0.0(0.0)     0.0(0.0) init
    2    0 S     20   1    0.0(0.0)     0.0(0.0)     0.0(0.0)     0.0(0.0) kthreadd
    3    0 S   -100   0    0.0(0.0)     0.0(0.0)     0.0(0.0)     0.0(0.0) migration/0
    4    0 S     20   0    0.0(0.0)     0.0(0.0)     0.0(0.0)     0.0(0.0) ksoftirqd/0
    5    0 S   -100   1    0.0(0.0)     0.0(0.0)     0.0(0.0)     0.0(0.0) migration/1

 --More--
```

The following example displays the tasks listed in ascending order of task IDs without displaying the tasks with 0 CPU usage within 15 minutes.

```
FS# show processes cpu nonzero
```

Description of the information displayed in this command:

Field	Description
System Uptime	Total running time of the device, precious to seconds.
CPU Utilization	Total CPU usage of the control core within the last five seconds, one minute, and five minutes.
Virtual CPU usage	Total CPU usage of the virtual control core within the last five seconds, one minute, and five minutes.
Tasks Statistics	Task statistics information, including the total number of statistics tasks and the task status.
set system cpu watermark	CPU watermark value and status of the control core.

The task running statuses are listed below:

Task Running Status	Description
running	Running task
sleeping	Suspended task
stopped	Stopped task
zombie	Terminated task, but not reclaimed by the system

Description of each task:

Field	Description
Pid	Task ID
Vsd	VSD ID
S	Task status. Five statuses in total: R (running), T (stopped), S (sleeping), D (waiting), and Z (zombie).
PRI	Task running priority
P	The core of the CPU on which the task runs
5sec/1min/5min/15min	CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs.
Process	Task name. Only the first 15 characters are displayed. The remaining characters are truncated.

The following example displays the CPU usage in ascending order of task IDs and only the processes with non-zero CPU usage within 15 minutes are displayed.

```
FS #show processes cpu nonzero
```

The following example displays the CPU usage in descending order within five seconds and the tasks with zero CPU usage within one second are not displayed.

```
FS #show processes cpu 5sec nonzero
```

The following example displays the CPU usage of the control core in histograms within the last 60 seconds, 60 minutes, and 72 hours.

The first histogram displays the CPU usage of the control core within 300 seconds. Every segment in the x-coordinate is five seconds, and every segment in the y-coordinate is 5%. The symbol "*" indicates the CPU usage at the last specified second. In other words, the first segment on the x-coordinate nearest to 0 is the CPU usage in the last five seconds, measured in %.

The second histogram displays the CPU usage of the control core within the last 60 minutes, measured in %. Every segment on the x-coordinate is 1 minute.

The third histogram displays the CPU usage of the control core within the last 72 hours, measured in %. Every segment on the x-coordinate is 1 hour.

Example:

```
FS#show processes cpu history

                    system cpu percent usage(%) [last 300 second]

     _
  100|
   95|
   90|
   85|
   80|
   75|
   70|
   65|
   60|
   55|
   50|
   45|
   40|*********
   35||||||||||
   30||||||||||*
   25|||||||||||
   20|||||||||||
   15|||||||||||
   10|||||||||||
    5|||||||||||***************
    0||||||||||||||||||||||||||
     #=========#=========#=====*==>
     0         50        100      second
          system cpu percent usage(%) per 5second (last 125 second)
--------------------------------------------------------------------------------



                 system cpu percent usage(%) [last 60 minute]

     _
  100|
   95|
   90|
   85|
   80|
   75|
   70|
   65|
   60|
   55|
   50|
   45|
   40|
   35|
   30|*
   25||
   20||
   15||
   10||
    5||*
    0|||
     #==*==>
```

```
      0          minute
               system cpu percent usage(%) per 1minute (last 2 minute)
--------------------------------------------------------------------------------
```

The following example displays the CPU usage of the core 0 in tables within the last 60 seconds, 60 minutes, and 72 hours.

The first table lists the CPU usage within 300 seconds. The first cell indicates the CPU usage within the last five seconds.

The second table lists the CPU usage within the last 60 minutes, measured in %. The two adjacent cells show the CPU usage measured at an interval of one minute.

The third table lists the CPU usage within the last 72 hours, measured in %. The two adjacent cells show the CPU usage measured at an interval of one hour.

Example:

```
FS #show processes cpu history table
                    system cpu percent usage(%) [last 300 second]
#-----------------------------------------------------------------------------#
|           |      1|      2|      3|      4|      5|      6|      7|      8|      9|     10|
#-----------------------------------------------------------------------------#
#-----------------------------------------------------------------------------#
|          0|    2.0|    2.4|    2.3|    2.3|    2.8|    3.0|    2.7|    3.2|    2.6|    2.4|
#-----------------------------------------------------------------------------#
|          1|    2.7|    2.5|    2.7|    2.2|    2.4|    2.6|    2.2|    2.7|    2.3|    2.5|
#-----------------------------------------------------------------------------#
|          2|    2.9|    2.0|    2.4|    2.5|    2.7|    2.4|    2.4|    2.6|    2.6|    2.5|
#-----------------------------------------------------------------------------#
|          3|    2.7|    2.8|    2.8|    3.2|    2.5|    3.2|    3.1|    4.0|    2.7|    2.7|
#-----------------------------------------------------------------------------#
|          4|    4.0|    2.3|    2.1|    2.2|    2.7|    2.4|    2.5|    2.6|    2.4|    2.6|
#-----------------------------------------------------------------------------#
|          5|    2.4|    3.2|    2.5|    2.3|    2.3|    3.6|    2.8|    2.5|    2.2|    2.4|
#-----------------------------------------------------------------------------#

                    system cpu percent usage(%) [last 60 minute]
#-----------------------------------------------------------------------------#
|           |      1|      2|      3|      4|      5|      6|      7|      8|      9|     10|
#-----------------------------------------------------------------------------#
#-----------------------------------------------------------------------------#
|          0|    2.6|    2.5|    3.0|    2.4|    2.6|
#-----------------------------------------------------------------------------#
```

Prompt Message -

Platform Description -

3.17 show processes cpu detailed

Use this command to display the details of the specified task.

show processes cpu detailed { *process-id* | process-*name* }

Parameter Description

Parameter	**Description**
process-id	Displays the information on the task of the specified task ID.
process-name	Displays the information on the task of the specified task name.

Command Mode

Privileged EXEC mode/ global configuration mode

Default Level

-

Usage Guide

This command is supported only in VSD0 mode. Multiple VSDs are not supported.

Configuration Examples

The following example displays the information on the task of the specified task name.

```
FS# show processes cpu detailed demo
Process Id      : 1820
Process Name    : demo
Vsdid           : 0
Process Ppid    : 1

State           : R(running)
On CPU          : 0
Priority        : 20
Age Time        : 24:06.5
Run Time        : 00:01.0
Cpu Usage       :
    Lass   5 sec     0.3% (0.6%)
    Lass   1 min     0.3% (0.6%)
    Lass   5 min     0.3% (0.6%)
    Lass  15 min     0.3% (0.6%)
Tty             : ?
```

ℹ Code Usage: 209.6 KB. If the specified task name is not unique, the system displays the following message:

```
FS# show processes cpu detailed demo
duplicate process, choose one by id not name.
name: demo, id: 1089, state: S(sleeping)
name: demo, id: 1091, state: R(running)
process name: monitor_procps, do NOT exist, or NOT only one.
```

Description of the displayed information:

Field	Description
Process Id	Task ID
Vsdid	VSD ID of the task
Process Name	Task name
Process Ppid	Parent process task ID
State	Task running status
On CPU	CPU where the task is running
Priority	Task priority
Age Time	Duration for the task from self-startup to now
Run Time	Duration for the task from self-startup to being executed
Cpu Usage	CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs. For example, the demo task is running on No.0 core, which is the control core and the system has two control cores. In this case, the CPU usage is 0.3% (0.6%).
Tty	Tty ID, in the format of "Primary device ID, secondary device ID". If it is 0, the value is **?**.
Code Usage	Size occupied by the task code segment

The following example displays the information on the task of the specified task ID.

```
FS# show process cpu detailed 1715
```

Prompt Message -

Platform Description -

3.18 show usb-bus

Use this command to display the information on the device mounted to the USB bus.

show usb-bus

Parameter Description

Parameter	**Description**
-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level -

Usage Guide -

Configuration Examples

1: The following example displays the information on the device mounted to the USB bus.

```
FS# show usb-bus
Device: Linux Foundation 2.0 root hub
   Bus 001 Device 001: ID 1d6b:0002
```

Prompt Message

-

Platform Description

-

3.19 show version

Use this command to display the system version information.

show version

Parameter Description

Parameter	Description
-	-

Command Mode

Privileged EXEC mode/ global configuration mode

Default Level

-

Usage Guide

-

Usage Guide

The following example displays the system version information.

```
FS# show version
System description           : FS Indoor AP320-I (802.11a/n and 802.11b/g/n) By FS Networks
System start time            : 2012-12-06 00:00:00
System uptime                   : 0:03:20:07
System hardware version : 1.0.0
System software version : AP_FSOS11.0(1B1)
System serial number        : 1234942570018
System boot version          : 1.0.0
```

Prompt Message

-

Platform Description

-

4 User Task Commands

4.1 clear user-task

Use this command to clear user task logs.

clear user-task

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 15

Usage Guide This command is used to clear user task logs.

Configuration Examples #Clear user task logs.

```
FS# clear user-task
```

4.2 show user-task

Use this command to display user task information.

show user-task [**log**]

Parameter Description

Parameter	Description
log	Queries user task information.

Command Mode Privileged EXEC mode and global configuration mode

Default Level 15

Usage Guide This command is used to display user task list and user task logs.

Configuration Examples #Display the list of all user tasks.

```
FS#sh user-task
User-task: enable
User-task log: enable
Time                    Name                    Mode      Loop Command-sequence
2014-09-22 15:00 Delete static binding relationship        config --     ip dhcp pool my_pool
no host
```

Field description: Field	Description
Time	Task time
Name	Task name
Mode	Command mode
Loop	Specifies whether to recycle a task and specifies the cycling interval.
Command-sequence	CLI command sequence to be run

#Display user task log information.

```
FS# configure terminal
FS(config)# user-task log enable
FS(config)# exit
FS# show user-task log
```

Prompt Information

```
--------------------
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
```

4.3 user-task

Use this command to add user tasks.

user-task add *task-name* **command** *cli-string* **mode** { **exec** | **config** } [**date** *YYYY MM DD*] **time** *hh:mm* [**every** { *mmm* |

hhh:mm }

Use the **no** form of this command to delete user tasks.

user-task delete *task-name*

Use this command to modify user tasks.

user-task modify *task-name* { **mode** { **exec** | **config** } | **date** *YYYY MM DD* | **time** *hh:mm* | **every** { *mmm* | *hhh:mm* }

Parameter Description

Parameter	Description
task-name	Specifies a task name. A task name cannot be longer than 16 bytes.
command *cli-string*	Specifies a CLI command sequence to be run. The total length of the sequence cannot exceed 512 bytes. ⚠ If a command contains space, use double quotation marks to include the command. ⚠ Sub-commands are separated using the symbol @. ℹ Commands can be abbreviated, for example, sh ip int br. 1. If a command contains the symbol @, use \@ instead.
mode { **exec** | **config** }	Specifies a command mode. **exec** indicates the privileged EXEC mode and **config** indicates the global configuration mode.
date *YYYY MM DD*	Specifies the task date. If no task date is specified, this parameter is set to the current day by default. ℹ If no task date is configured and the task time is earlier than current time, this parameter is set to the next day by default.
time *hh:mm*	Specifies task time, in the range from 00:00 to 23:59 ❗ If the configured task date and time is earlier than the current date and time, the configured commands will be run immediately, including the **reload** command.
every { *mmm* | *hhh:mm* }	Specifies task interval. The range is from 1 minute to 168 hours (namely, 1 minute to 1 week). After a task interval is configured, tasks will be run at the specified interval. If no task interval is configured, tasks will not be repeatedly run. ℹ Example: 999 (min) and 167:59 (167 hr and 59 min)

Command Mode

Privileged EXEC mode

⚠ This command must be run in privileged EXEC mode.

Default Level

15

Usage Guide

This command is used to add, delete, or modify user tasks. An added task will be stored in the task database. The system will run tasks according to task time. To delete or modify a task, specify a task name. If multiple attributes of a task need to be modified, you should modify the attributes one after another. Only one attribute can be modified at a time.

Configuration Examples

#Add a user task which specifies that devices should be restarted at 4:30 p.m. on Sept. 2, 2014.

```
FS# user-task add reload-task command “reload@y” mode exec date 2014 9 2 time 16:30
```

#Delete a task named test.

```
FS# user-task delete test
```

#Change the time of a non-cyclic task named aa to 12:00 p.m. each day.

```
FS# user-task modify aa every 24:00
FS# user-task modify aa time 12:00
```

Prompt Information

1. If the entered task name is too long, configuration fails, and the following message is displayed:

```
USER-TASK: Task name len 22 is more than 16 bytes!
```

2. If the entered command is too long, configuration fails, and the following message is displayed:

```
USER-TASK: Command len 567 is more than 512 bytes!
```

3. If the entered task name already exists, task adding fails, and the following message is displayed:

```
USER-TASK: Task name exists!
```

4. If the entered task name does not exist, task deletion/modification fails, and the following message is displayed:

```
USER-TASK: No such task named test!
```

5. If the entered date and time is earlier than the current date and time, task time/data modification fails, and the following message is displayed:

```
USER-TASK: New time is less than current time!
```

6. If an exception occurs to the database, configuration fails, and the following message is displayed:

```
USER-TASK: Unexpected database error!
```

7. If the number of tasks is greater than 1000, task adding fails, and the following message is displayed:

```
USER-TASK: Too more tasks!(Not support more than %d tasks)
```

Common Errors

Configuration fails if parameters of a command are not included using quotation marks.

4.4 user-task enable

Use this command to enable the user task function.

user-task enable

Use the **no** form of this command to disable the user task function.

no user-task enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The user task function is enabled by default.

Command Mode Global configuration mode

Default Level 15

Usage Guide With the user task function enabled, you can run the user-defined commands in the task database.

⚠ If tasks fail to be run in a timely manner due to reasons such as device restart or user task being disabled, or there are tasks in the task database earlier than the current tasks, these timed-out tasks will be run first after the user task function is enabled. For cyclic tasks, task time is calculated based on the task plan time and cycling interval.

Configuration Examples #Enable the user task function.

```
FS(config)# user-task enable
```

Verification 1. Run the **show user-task** command to check whether the user task function is enabled.

2. Run the **show run** command to check whether the user task function is enabled.

4.5 user-task log

Use this command to enable the user task log function.

user-task log enable

Use the **no** form of this command to disable the user task log function.

no user-task log enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The user task log function is disabled by default.

Command Mode Global configuration mode

Default Level 15

Usage Guide

If the tasks to be configured include **show** commands which will provide task results after the commands are run, the task log function must be enabled to record task execution results.

⚠ Logs can be stored for 30 days at most.

⚠ Maximum log size is 20 MB.

Configuration Examples

#Enable the user task log function.

```
FS(config)# user-task log enable
```

Verification

1. Run the **show user-task** command to check whether the user task function is enabled.

2. Run the **show run** command to check whether the user task function is enabled.

5 SERVICE-MANAGER Commands

5.1 servctl service

Use this command to set the service status. Use the **no** form of this command to restore the default service status.

servctl service *name* { **on** | **off** }

no servctl service *name*

Parameter Description

Parameter	Description
name	Specifies the service name.
on	Sets the service status to Running.
off	Sets the service status to Stop.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to set the running status of services on a device, control whether the related service modules are loaded upon device startup, and determine whether to display corresponding web pages.

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 Examples

The following example enables the was service to run upon device startup.

```
FS(config)#servctl service was on
```

Prompt Message

Prompts are displayed based on the service loading or unloading status. Loading or unloading some services takes effect after the device is restarted.

You must reload the system to enable service was.

5.2 show servctl

Use this command to display services that can be controlled by Service Manager and the service status.

show servctl { **all | service** *name* }

Parameter Description

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

Default Level 14

Usage Guide Use this command to display services that can be controlled by Service Manager and the service status.

Configuration Examples The following example displays the status of the was service.

```
FS#show servctl service was
service              controllable startup    running
------------------- ------------ --------- ---------
was                    true          true       true
```

Field description:

Field	Description
service	Indicates the service name
controllable	Indicates whether a service can be controlled for loading or unloading.
startup	Indicates whether a service is set to running upon device startup.
running	Indicates whether a service is running.

Prompt Message If the service name does not exist, only the titles are displayed.

```
FS#show servctl service foo
service              controllable startup    running
------------------- ------------ --------- ---------
```

Chapter 5 Interface Commands

1 Interface Commands

1.1 bandwidth

Use this command to set the bandwidth on the interface. Use the **no** form of this command to restore the default setting.

bandwidth *kilobits*

no bandwidth

Parameter Description

Parameter	Description
kilobits	Bandwidth per second, in the unit of Kbps.

Defaults

If this command is not configured on the interface, use the show interface command to display the default setting in privileged EXEC mode.

Command Mode

Interface configuration mode

Usage Guide

This command does not affect the actual bandwidth on the interface. Instead, it is used to display the system the bandwidth specification. By default, the bandwidth is determined by the actual link rate on the interface. It can be set by the user as well.

Configuration Examples

The following example sets the bandwidth on the interface to 64 Kbps.

```
FS(config)#interface gigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# bandwidth 64
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.2 carrier-delay

Use this command to set the carrier delay on the interface. Use the no form of this command to restore the default value.

carrier-delay { [milliseconds] num | up [milliseconds] num down [milliseconds] num}

no carrier-delay

Parameter Description

Parameter	Description
num	(Optional) in the range from 0 to 60 in the unit of seconds.

milliseconds	(Optional) in the range from 0 to 60000 in the unit of milliseconds.
up	(Optional) Configures the delay after which DCD changes from Down to Up in status.
down	(Optional) Configures the delay after which DCD changes from Up to Down in status.

Defaults The default is 2 seconds.

Command Mode Interface configuration mode

Usage Guide This parameter refers to the delay after which the carrier detection signal DCD of the interface link changes from the Down status to the Up status or vice versa. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upper data link layer for renegotiation.

If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route aggregation so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is shorter than the time used for route aggregation, you should set the parameter to a higher value to avoid unnecessary route vibration.

Configuration Examples The following example sets the carrier delay of serial interface to 5 seconds.

```
FS(config)# interface gigabitethernet 1/1
FS(config)# carrier-delay 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.3 clear counters

Use this command to clear the counters on the specified interface.

clear counters [*interface-id*]

Parameter Description

Parameter	Description
interface-id	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide

In the privileged EXEC mode, use the **show interfaces** command to display the counters or the **clear counters** command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.

Configuration Examples

The following example clears the counters on interface gigabitethernet 1/1.

```
FS# clear counters gigabitethernet 1/1
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description

N/A

1.4 clear interface

Use this command to reset the interface.

clear interface *interface-id*

Parameter Description

Parameter	Description
interface-id	Interface type and interface ID

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

This command is only used on the switch port, member port of the L2 Aggregate port, routing port, and member port of the L3 aggregate port. This command is equal to the **shutdown** and **no shutdown** commands.

Configuration Examples

The following example resets the interface gigabitethernet 1/1.

```
FS# clear interface gigabitethernet 1/1
```

Related Commands

Command	Description
shutdown	Disables the interface.

Platform Description

N/A

1.5 description

Use this command to configure the alias of interface. Use the **no** form of this command to restore the default setting.

description *string*

no description

Parameter Description

Parameter	Description
string	Interface alias

Defaults

No alias is configured by default.

Command Mode

Interface configuration mode.

Usage Guide

Use **show interfaces** to display the interface information, including the alias.

Configuration Examples

The following example configures the alias of interface.

```
FS(config)# interface gigabitethernet 1/1
FS(config-if)# description GBIC-1
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description

N/A

1.6 duplex

Use this command to specify the duplex mode for the interface. Use the **no** form of this command to restore the default setting.

duplex { **auto** | **full** | **half** }

no duplex

Parameter Description

Parameter	Description
auto	Self-adaptive full duplex and half duplex
full	Full duplex
half	Half duplex

Defaults

The default is **auto**,

Command Mode

Interface configuration mode.

Usage Guide

The duplex mode is associated with the interface type. Use **show interfaces** to display the duplex mode of the interface

Configuration Examples

The following example specifies the duplex mode for the interface.

```
FS(config-if)# duplex full
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description

N/A

1.7 interface

Use this command to enter the interface configuration mode.

interface *interface-type interface-number*

Parameter Description

Parameter	Description
interface-type	The interface type.
interface-number	The interface ID.

Defaults

N/A

Command Mode

Interface configuration mode

Usage Guide

This command is used to enter interface configuration mode. The user can modify the interface configuration next,

Configuration Examples

The following example enters configuration mode on Aggregateport 1.

```
FS(config)# interface Aggregateport 1
FS(config-if-Aggregateport 1)#
```

The following example enters configuration mode on GigabitEthernet 1/2.

```
FS(config)# interface GigabitEthernet 1/2
FS(config-if-GigabitEthernet 1/2)#
```

The following example configuration mode on VLAN 1.

```
FS(config)# interface vlan 1
FS(config-if-VLAN 1)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.8 interface range

Use this command to enter interface configuration mode on multiple interfaces.

interface range { *port-range* | **macro** *macro_name* }

Use this command to define the macro name of the **interface range** command.

define interface-range *macro_name*

Parameter Description

Parameter	Description
port-range	The interface type and ID range, entered in the form of *interface-type slot-number/interface-number*. The interface can be either an Ethernet physical interface or a loopback interface.
macro *macro_name*	The macro name which represents the interface range.

Defaults The **interface range** command is disabled by default.

Command Mode Global configuration mode

Usage Guide Use the define interface-range command to define a range of interfaces as the macro name and then use the **interface** range macro macro_name command to enter interface configuration mode on multiple interfaces.

Configuration Examples The following example enters interface configuration mode on multiple interfaces by setting the interface range.

```
FS(config)# interface range gigabitEthernet 0/0, 0/2
FS(config-if-range)# bandwidth 100
```

The following example enters interface configuration mode on multiple interfaces by defining the macro name.

```
FS(config)# define interface-range route1 gigabitEthernet 0/0-2
FS(config)# interface range macro route1
FS(config-if-range)# bandwidth 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.9 load-interval

Use this command to set the interval for calculating load on the interface. Use the **no** form of this command to restore the default setting.

load-interval *seconds*

no load-interval

Parameter Description

Parameter	Description
seconds	In the range from 5 to 600 in the unit of seconds.

Defaults The default is 10.

Command Mode Interface configuration mode

Usage Guide This command is used to set the interval for calculating load on the interface. In general, the numbers of incoming and outgoing packets and bytes are calculated every 10 seconds. For example, if the parameter is set to 180 seconds, the following outcome is displayed when the **show interface gigabitEthernet 0/1** command is run.

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

Configuration Examples The following example sets the interval for calculating load on interface GigabitEthernet 0/1 to 180 seconds.

```
FS(config)# interface gigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# load-interval 180
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.10 logging

Use this command to print information on the interface. Use the no form of this command to disable this function.

logging [**link-updown** | **error-frame** | **link-dither**]

no logging [**link-updown** | **error-frame** | **link-dither**]

Parameter Description

Parameter	Description
link-updown	Prints the status change information.
error-frame	Prints the error frame information.
link-dither	Prints the oscillation information.

Defaults This function is enabled by default.

Command Global configuration mode

Mode

Usage Guide N/A

Configuration Examples

The following example prints information on the interface..

```
FS(config)# logging link-updown
FS(config)# logging error-frame
FS(config)# logging link-dither
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.11 medium-type

Use this command to specify the medium type for an interface. Use the **no** form of this command to restore the default setting.

medium-type { **auto-select** [**prefer** [**fiber | copper**]] **| fiber** | **copper** }

no medium-type

Parameter Description

Parameter	Description
fiber	Optical interface.
prefer [**fiber** | **copper**]	The preferred medium type for the interface is selected.
auto-select	Auto-selects the medium type for the interface.
copper	Copper interface.

Defaults The default is **copper**.

Command Mode Interface configuration (physical interface, except for AP and SVI)

Usage Guide If a port can be selected as an optical port or electrical port, you can only select one of them. Once the media type is selected, the attributes of the port, for example, status, duplex, flow control, and rate, all mean those of the currently selected media type. After the port type is changed, the attributes of the new port type take the default values, which can be modified as needed.

Configuration Examples

The following example specifies the medium type for interface gigabitethernet 1/1.

```
FS(config)# interface gigabitethernet 1/1
FS(config-if)# medium-type copeer
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description

The 12 SFP interfaces of the 24SFP/12GT line cards and 1210/100/1000M BASE-T interfaces allow for dynamic switching.

The combo interface is not supported to automatically determine whether the current port is the SFP interface or the 10/100/1000M BASE-T interface.

1.12 mtu

Use this command to set the MTU supported on the interface.

mtu *num*

Parameter Description

Parameter	Description
num	64 to 9216 (or 65536, which varies by products)

Defaults

The default is 1500.

Command Mode

Interface configuration mode.

Usage Guide

This command is used to set the maximum transmission unit (MTU) supported on the interface.

Configuration Examples

The following example sets the MTU supported on interface gigabitethernet 1/1 to 9000.

```
FS(config)# interface GigabitEthernet 1/1
FS(config-if-GigabitEthernet)# mtu 9000
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description

N/A

1.13 physical-port dither protect

Use this command to enable oscillation protection on the port. Use the **no** form of this command to disable this function.

physical-port dither protect

no physical-port dither protect

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide After you configure the **physical-port dither protect** command, the port will be shut down when the oscillation occurs for certain times.

ⓘ If oscillation occurs on the port for 6 times within 2 seconds, a syslog will be printed. If syslog is printed for 10 consecutive times, the port will be shut down, If oscillation occurs on the port for over 10 times within 10 seconds, a syslog will be printed but the port will not be shut down.

Configuration Examples The following example enables oscillation protection on the port.

```
FS(config)# physical-port dither protect
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.14 show interfaces

Use this command to display the interface information and optical module information.

show interfaces [*interface-type interface-number*] [**description**]

Parameter Description

Parameter	Description
interface-id *interface-number*	Interface (including Ethernet interface, aggregate port, SVI or loopback interface).
description	The description of the interface, including the link status.

Defaults All interface information is displayed by default.

Command Mode Privileged EXEC mode.

Usage Guide This command is used to show all basic information if no parameter is specified.

Configuration

Examples

The following example displays the interface information when the Gi0/1 is an Access port.

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN     , line protocol is DOWN
  Hardware is Broadcom 5464 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 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
    Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: access
    Vlan id : 2
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Rxload is 1/255, Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

The following example displays the layer-2 interface information when the Gi0/1 is a Hybrid port.

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN     , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet
  Interface address is: no ip address
  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
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
  Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
  Priority is 0
  Medium-type is Copper
  Admin duplex mode is AUTO, oper duplex is Unknown
  Admin speed is AUTO, oper speed is Unknown
  Flow receive control admin status is OFF,flow send control admin status is OFF
  Flow receive control oper status is Unknown,flow send control oper status is Unknown
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Bridge attributes:
  Port-type: hybrid
  Tagged vlan id:2
  Untagged vlan id:none
Queueing strategy: FIFO
  Output queue 0/0, 0 drops;
  Input queue 0/75, 0 drops
Rxload is 1/255 ,Txload is 1/255
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  0 packets output, 0 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
```

Related Commands

Command	**Description**
duplex	Duplex
flowcontrol	Flow control status.
interface gigabitEthernet	Selects the interface and enter the interface configuration mode.
interface aggregateport	Creates or accesses the aggregate port, and enters the interface configuration mode.
interface vlan	Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode.
shutdown	Disables the interface.
speed	Configures the speed on the port.
switchport priority	Configures the default 802.1q interface priority.

switchport protected	Configures the interface as a protected port.

Platform Description

N/A

1.15 show interfaces link-state-change statistics

Use this command to display the link state change statistics, including the time and count.

show interfaces [*interface-type interface-number*] **link-state-change statistics**

Parameter Description

Parameter	Description
interface-type interface-number	The interface type and ID.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

If you do not specify an interface, the link state statistics of all interfaces are displayed.

Configuration Examples

The following example displays the link state statistics of interface GigabitEthernet 0/1.

```
FS# show interfaces GigabitEthernet 0/1 link-state-change statistics
Interface     Link state     Link state change times     Last change time
------------  ---------      -----------------------     -------------------
Gi 0/1        down           100                                        2012-12-24 15:00:00
```

Interface	Description
Link state	Current link state.
Link state change times	The count of link state change.
Last change time	The time when the last link state change occurs.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.16 show interfaces status

Use this command to display interface status information.

show interfaces [*interface-type interface-number*] **status**

Parameter Description

Parameter	Description
interface-type interface-number	The interface type and ID.
status	Displays interface status information, including speed and duplex.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

If you do not specify an interface, the status information of all interfaces is displayed.

Configuration Examples

The following example displays the status information of interface GigabitEthernet 0/1.

```
FS#show interfaces GigabitEthernet 0/1 status
Interface                    Status          Vlan       Duplex   Speed    Type
--------------------     ----------     ------     ------   ------   ------
GigabitEthernet 0/1       up                  1            Full      1000M     copper
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.17 show interfaces usage

Use this command to display bandwidth usage of the interface.

show interfaces [*interface-type interface-number*] **usage** [*up* | *down*]

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) The interface type and ID.
up	(Optional) Displays the port up statistics.
down	(Optional) Displays the port down statistics.

Defaults

N/A

Command Mode

Any CLI mode

Usage Guide

If you do not specify an interface, the bandwidth usage of all interfaces is displayed. Bandwidth refers to the actual link bandwidth rather than the *bandwidth* parameter configured on the interface.

Configuration Examples

The following example displays bandwidth usage of interface GigabitEthernet 0/1.

```
Interface                      Bandwidth     Average Usage      Output Usage      Input Usage
---------------------------- ------------- ------------------ ----------------- -----------------
GigabitEthernet 0/0            1000 Mbit     0.002822759%       0.001183280%      0.004462237%
```

Bandwidth refers to the interface link bandwidth, the maximum speed of link. Average Usage refers to the current usage.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.18 shutdown

Use this command to disable an interface. Use the **no** form of this command to enable a disabled port.

shutdown

no shutdown

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the administrative status of an interface is Up.

Command Mode

Interface configuration mode

Usage Guide

Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the **no shutdown** command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

If you use the script to run no shutdown frequently and rapidly, the system may prompt the interface status reversal.

Configuration Examples

The following example disables an interface.

```
FS(config)# interface aggregateport 1
FS(config-if)# shutdown
```

The following example enables an interface.

```
FS(config)# interface aggregateport 1
FS(config-if)# no shutdown
```

Related Commands

Command	Description
clear interface	Resets the hardware.
show interfaces	Displays the interface information.

Platform Description N/A

1.19 snmp trap link-status

Use this command to send LinkTrap on a port. Use the **no** form of this command to disable this function.

snmp trap link-status

no snmp trap link-status

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default

Command Mode Interface configuration mode.

Usage Guide For an interface (for instance, Ethernet interface, AP interface, and SVI interface), this command sets whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.

Configuration Examples The following example disables the interface from sending LinkTrap on the interface.

```
FS(config)# interface gigabitEthernet 1/1
FS(config-if)# no snmp trap link-status
```

The following example enables the interface to forward Link trap.

```
FS(config)# interface gigabitEthernet 1/1
FS(config-if)# snmp trap link-status
```

Related Commands

Command	Description
snmp trap link-status	Enables the interface to send LinkTrap on the interface.
no snmp trap link-status	Disables the interface from sending LinkTrap on the interface.

Platform Description N/A

1.20 snmp-server if-index persist

Use this command to set the interface index persistence. The interface index remains the same after the device is restarted.

snmp-server if-index persist

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide After this command is configured, all interface indexes are saved in the configuration file. After the device is restarted, interface indexes remain the same as before.

Configuration Examples The following example enables the interface index persistence.

```
FS(config)# snmp-server if-index persist
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.21 speed

Use this command to configure the speed on the port. Use the **no** form of this command to restore the default setting.

speed [**10** | **100** | **1000** | **auto**]

Parameter Description

Parameter	Description
10	The transmission rate of the interface is 10Mbps.
100	The transmission rate of the interface is 100Mbps.
1000	The transmission rate of the interface is 1000Mbps.
auto	Self-adaptive

Defaults The default is **auto**.

Command Interface configuration mode.

Mode

Usage Guide

If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use **show interfaces** to display configuration. The rate varies by interface types. For example, you cannot set the rate of a SFP interface to 10M or 100M.

Configuration Examples

The following example sets the speed on interface gigabitethernet 1/1 to 100Mbps.

```
FS(config)# interface gigabitethernet 1/1
FS(config-if)# speed 100
```

Related Commands

Command	**Description**
show interfaces	Displays the interface information.

Platform Description

N/A

2 Mode Management Commands

2.1 bridge-map

Use this command to enter the bridge-map command mode layer.

bridge-map *bridge-num*

Parameter Description

Parameter	Description
bridge-map *bridge-num*	Bridge-map index. Its value depends on the number of network interfaces on the device. In the bridge configuration, an inside interface and an outside interface are required to form a pair of bridges. Therefore, the number of inside-outside interface pairs equals that of bridge-maps. Sub-interfaces are not counted in the inside-outside interface pairs because bridges cannot be configured on sub-interfaces. For example, if the device has a maximum of three inside-outside interface pairs, the bridge-map index ranges from 0 to 2.

Defaults

N/A.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

By configuring this command, you will enter the bridge-map command mode layer, where you can specify the bridge-map and operating mode of inside and outside interfaces.

⚠ You must switch to a non-gateway mode to configure this command. For details about the command for switching to a non-gateway mode, see sys-mode.

⚠ You cannot use the **no** form of this command for the bridge-map command mode layer.

Configuration Examples

1. #Enter the bridge-map command mode layer.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#bridge-map 0
FS(config-bridge-map)#
```

Verification

1. You can use the **show bridge-map** command to view information about the bridge-maps supported on the current device.

Prompt Information

1. You enter the bridge-map command mode layer after specifying valid parameters.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#bridge-map 0
FS(config-bridge-map)#
```

2. If you enter invalid parameters, the system prompts that the current bridge does not exist.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#bridge-map 5
%% Bridge 5 not exist!
```

3. If you use the **no** form of this command, the system prompts that it is not permitted.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#no bridge-map 5
%% Removal of bridge-map is not permitted
```

Platform Description

This command is supported only in the bridging mode.

2.2 bypass couple

Use this command to enable a specified hardware bypass pair.

bypass couple *couple-num*

Use the **no** form of this command to restore the default setting.

no bypass couple *couple-num*

Parameter Description

Parameter	Description
couple-num	Specifies a hardware bypass pair to be enabled.

Defaults

The hardware bypass function is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to enable a specified hardware bypass pair.

Configuration Examples

1. # Configure the first hardware electrical port bypass pair (numbered 0) of a device.

```
FS(config)# bypass couple 0
```

Verification

You can use the **show running-config** command to view the configuration result.

Prompt Information

1: If the configured mode is the same as the current mode, there is not any prompt information.

2: If the configured mode is different from the current mode, the prompt is as follows when

the hardware bypass function starts

```
Couple 0 bypass started.
```

The hardware bypass function stops

```
Couple 0 bypass stoped.
```

Prompts starting with “error” are error warnings.

Platform Description

1. There is one bypass pair on EG2000D/EG2000T/EG2000CE/EG2000SE/EG2000P, namely, couple 0 (composed by GigabitEthernet 0/5 and GigabitEthernet 0/6).
2. There are two bypass pairs on EG2000G/EG2000GE/ACE2000E, namely, couple 0 (composed by GigabitEthernet 0/2 and GigabitEthernet 0/4) and couple 1 (composed by GigabitEthernet 0/3 and GigabitEthernet 0/5).
3. There are two bypass pairs on EG2000X/EG2000XE/EG2000UE/ACE3000E, namely, couple 0 (composed by GigabitEthernet 0/0 and GigabitEthernet 0/1) and couple 1 (composed by GigabitEthernet 0/2 and GigabitEthernet 0/3).
4. This command is only supported on the above-mentioned products.

2.3 write-db enable

Use this command to enable the function of not storing logs in the local hard disk.

no write-db enable

Use the **no** form of this command to disable the function of not storing logs in the local hard disk.

write-db enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

On EG2000X/XE/UE and ACE3000E, the function of not storing logs in the local hard disk is enabled by default. EG2000G/GE and ACE2000E, the function of not storing logs in the local hard disk is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to enable the function of not storing logs in the local hard disk. Save the configuration and restart the device before the configuration takes effect.

After enabling the function of not storing logs in the local hard disk, logs, such as audit, traffic audit, content audit, and flow logs are not stored in the local hard disk

Configuration Examples

1. # Enable the function of not storing logs in the local hard disk.

```
FS(config)#no write-db enable
```

Verification

Run the **show write-bd** command to verify whether this function takes effect.

Prompt Information

1. System reboot is required before the configuration takes effect.

```
FS#configure terminal

Enter configuration commands, one per line.    End with CNTL/Z.

FS(config)# no write-db enable

Write-db status has changed, you must save config and reload the system.
```

Platform Description

This command is only supported on EG2000X/XE/UE/G/GE, ACE3000E and ACE2000E.

2.4 convert

Use this command to switch Layer-2 port into Layer-3 port and specify initial internal and external network attributes.

convert port *num* **to { wan | lan }**

Use the **no** form of this command to SWITCH A Layer-3 port into a Layer-2 port.

no convert port *num*

Parameter Description

Parameter	Description
num	Indicates the port ID. The range is from 1 to 4.

Defaults

By default, all ports are Layer-2 ports.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1. Port 0 cannot be switched.
2. Store the configuration before it takes effect.

Configuration Examples

1. # Switch Port 2 into Layer-3 LAN port and switch Port 4 into Layer-3 WAN port

```
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)#exit
*Oct 23 10:35:29: %SYS-5-CONFIG_I: Configured from console by console
FS#write
```

```

Building configuration...


[OK]
FS#
```

Verification

Run the **show switch-info** command to display the configuration result.

```
FS#show switch-info
PORT0      LAN6      0
PORT1      PORT1     1
PORT2      LAN4      1
PORT3      PORT3     1
PORT4      WAN2       1

FS#
```

Prompt Information

1. Configuration succeeds. Save the configuration and reload the system.

```
##### Please save config and reload the system!!!!!
```

2. The port is already a Layer-3 port, the configuration does not take effect.

```
Error: Port 2 is already WAN port, this operation is invalid!
```

3. A Layer-2 port cannot be configured as a Layer-2 port. No prompts.

Common Error

The port is already a Layer-3 port, the configuration does not take effect.

Platform Description

N/A

2.5 lan-ip

Use this command to configure the IP address and mask of the internal network segment in receive-only mode.

lan-ip *ip_address subnet_mask*

Use this command to remove the IP address and mask of the internal network segment in receive-only mode.

no lan-ip *ip_address subnet_mask*

Parameter Description

Parameter	Description
ip_address	IP address of the internal network segment
subnet_mask	Mask of the internal network segment

Defaults

N/A.

Command Mode

Bridge-map command layer configuration mode

Default Level

14

Usage Guide

You can set the bridge in one-armed mode based on actual conditions of the internal network segment.

⚠ You must switch to a non-gateway mode to configure this command. For details about the command for switching to a non-gateway mode, see sys-mode.

⚠ In one-armed mode, you need to properly configure the IP address segment of the internal network to ensure proper operation of the transactions in this mode.

ℹ You can configure up to 100 network segments. The same network segment can be defined for two different one-armed modes.

Configuration Examples

1. #Configure bridge-map 0 operating in receive-only mode; the current network segments are 192.168.1.0/24 and 10.10.10.0/24.

```
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 192.168.1.0 255.255.255.0
FS(config-bridge-map)# lan-ip 10.10.10.0 255.255.255.0
```

Verification

1. You can use the **show bridge-map** *bridge-num* **lan-ip** command to view the internal network segment configuration of a specific bridge.

Prompt Information

1. If you configure the IP address segment of the internal network in non-one armed mode, the system prompts that such configuration is not permitted.

```
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)# lan-ip 192.168.1.0 255.255.255.0
it's not receive_only mode!
```

2. If you configure the 101st internal network segment, the system prompts that the IP address segment is full.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#bridge-map 0
FS(config-bridge-map)# lan-ip 192.168.101.0 255.255.255.0
lan ip net is full!
```

Platform Description

This command is supported only in the bridging mode.

2.6 link-mode

Use this command to configure the bridge-map and its operating mode.

link-mode *interface-name1 interface-name2* { **forward** | **sniffer** | **bypass** | **receive-only** }

Use this command to remove the configuration of the bridge-map and operating mode for inside and outside interfaces.

no link-mode *interface-name1 interface-name2* { **forward** | **sniffer** | **bypass** | **receive-only** }

Parameter Description

Parameter	Description
interface-name1	Inside interface of the bridge-map. This parameter cannot be configured for the outside interface.
interface-name2	Outside interface of the bridge-map. This parameter cannot be configured for the inside interface.
forward	The inside and outside interfaces corresponding to this bridge-map operate in *forward* mode, and they can implement traffic identification, blocking, control and auditing for forwarded packets.
sniffer	The inside and outside interfaces corresponding to this bridge-map operate in *sniffer* mode, and they can implement traffic identification and auditing for forwarded packets.
bypass	The inside and outside interfaces corresponding to this bridge-map operate in software *bypass* mode, and they directly forward packets after performing traffic statistics.
receive-only	The inside and outside interfaces corresponding to this bridging mode table operate in *receive-only* mode, and they can implement traffic identification and other operations on forwarded packets, but they only receive packets and do not forward packets.

Defaults

N/A.

Command Mode

Bridge-map command layer configuration mode

Default Level

14

Usage Guide

Bridging mode configuration is not supported on the sub-interface.

You can select the appropriate bridging mode based on your actual needs.

⚠ You must switch to a non-gateway mode to configure this command. For details about the command for switching to a non-gateway mode, see sys-mode.

Configuration Examples

1. #Configure the inside interface GigabitEthernet 0/0 and the outside interface GigabitEthernet 0/1 so that they operate in forward mode.

```
FS(config)#bridge-map 0
FS(config-bridge-map)#link-mode GigabitEthernet 0/0 GigabitEthernet 0/1 forward
```

Verification

1. You can use the **show bridge-map** command to view the current bridge configuration.

Prompt Information

1. Set the operating mode of the bridge-map to bypass.

```
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 bypass
```

2. If you repeat this command, the system prompts that new configuration will overwrite the existing one.

```
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
```

3. If the first interface is not an inside interface, or the second one is not an outside interface, or both interfaces are of the same type, the system displays the following prompt. Here we assume that Gi0/0 and Gi0/2 are inside interfaces and Gi0/1 is an outside interface.

```
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 0/1 GigabitEthernet 0/0 forward
%% Wan interface is not suitable for bridge-map inside interface, please use lan interface instead.

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 0/2 forward
%% Lan interface is not suitable for bridge-map ouside interface, please use wan interface instead.

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 0/0 forward
%% Inside interface can't be the same as outside interface.
```

4. If specified interface pairs are already in other bridge-maps, the system displays corresponding prompts.

```
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
%% Lan interface has configured on other bridge map.
```

```
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 0/2 GigabitEthernet 0/1 forward
%% Wan interface has configured on other bridge map.
```

Common Errors

1. The bridge comprises interfaces with incorrect attributes.
2. IP address segment of the internal network is not configured for the one-armed mode.

Platform Description

Other gateway products support four operating modes: orward, Sniffer, Software Bypass, and Single Arm modes.

This command is only supported in the bridge mode.

2.7 mirror

Use this command to enable port mirroring.

mirror master port *master_port* **slave port** *slave_port* **{ rx | tx | all }**

Use the **no** form of this command to restore the default setting.

no mirror master port *master_port* **slave port** *slave_port* **{ rx | tx | all }**

Parameter Description

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.

Defaults

By default, port mirroring is disabled.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1: Mirroring and mirrored ports should be Layer-2 ports.

2: There should be one and only mirroring port for each device.

Configuration Examples

1. # Mirror all packets on Port 1 to Port 0.

```
FS(config)#mirror master port 0 slave port 1 all
FS(config)#
```

2. #Mirror all packets received on Port 2 to Port 0.

```
FS(config)#mirror master port 0 slave port 2 rx
FS(config)#
```

3. #Mirror all packets sent on Port 3 to Port 0.

```
FS(config)#mirror master port 0 slave port 3 tx
FS(config)#
```

Verification

Run the **show mirror** command to display the configuration result.

```
master: 0
slave: 1(all) 2(rx) 3(tx)
```

Prompt Information

1. Configuration succeeds. No prompts.

2. The mirroring port is not a Layer-2 port. Wrong configuration.

```
Error: Master port must be lan port, port 1 is wan port!
```

3. The mirrored port is not a Layer-2 port. Wrong configuration.

```
Error: Slave port must be lan port, port 2 is wan port!
```

4. Port 1 has been set as the mirroring port. But during operation, the command for the mirroring port is mistakenly run on Port 2. Wrong configuration.

```
Error: Master port has been set to port 1 but not port 2!
```

5. The mirroring port and the mirrored port are the same port. Wrong configuration.

```
Error: Port 1 can not be mirrored to itself!
```

6. Delete a mirrored port, but no mirrored port has been set. Invalid command.

```
Warn: No mirrored port has been set!
```

7. Delete a mirrored port but the port has not been mirrored. Invalid command.

```
Warn: Port 2 has not been mirrored yet!
```

Common Errors

1: The mirrored port or the mirroring port is not a Layer-2 port.

2: The newly configured mirroring port is not the one configured before.

3: A port is configured both as the mirroring port and the mirrored port.

Platform Description

N/A

2.8 native

Use this command to configure native VLAN of a Layer-2 port.

native lan *num* **vid** *vlan-id*

Use the **no** form of this command to restore the default setting.

no native lan *num*

Parameter Description

Parameter	Description
num	Indicates the port ID. The value range is [0, 4].
vlan-id	Indicates the native VLAN to be set.

Defaults

By default, the native VLAN of all Layer-2 ports is VLAN 4089.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Before the command configuration, run the **vlan port** command to add the ports to the required VLAN (without any tag).

Configuration Examples

1. # 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
!
…
```

Prompt Information

1. Configuration succeeds. No prompts.

2. The port is a Layer-3 port, so the native VLAN cannot be set.

```
Error: Port 4 is WAN port, can't set native vlan!
```

3. The configured VLAN does not exist, because the VLAN is not encapsulated on a sub-interface in advance.

```
Error: Vlan 300 is unpresent!
```

4. The port is not in the configured VLAN.

```
Error: Port 3 is not in vlan 100!
```

5. The VLAN to be configured should be tagged while the native VLAN untagged.

```
Error: Vlan 100 is tag, the native vlan must be untag!6.
```

Common Errors

1: The port is a Layer-3 port, so the native VLAN cannot be set.

2: The configured VLAN does not exist, because the VLAN is not encapsulated on a sub-interface in advance.

3: The port is not in the configured VLAN.

4: The VLAN to be configured should be tagged while the native VLAN untagged.

Platform Description

N/A

2.9 native-vlan

Use this command to set the native-VLAN ID value of the bridge-map.

native-vlan *vlan-id*

Use this command to remove the native-VLAN ID value of the bridge-map.

no native-vlan

Use this command to restore the default configuration.

default native-vlan

Parameter Description

Parameter	Description
native-vlan *vlan-id*	VLAN ID value, in the range of 1~4094
default	The native-VLAN ID is 1 by default.

Defaults

The native-VLAN ID is 1 by default.

Command Mode

Bridge-map command layer configuration mode

Default Level

14

Usage Guide

In actual network environment, if the bridge receives a packet without vlan tag, the packet is identified as a VLAN classification object corresponding to the currently configured VLAN ID; if the packet has a VLAN tag, it is identified as a VLAN classification object corresponding to the tag.

⚠ You must switch to a non-gateway mode to configure this command. For details about the command for switching to a non-gateway mode, see sys-mode.

Configuration Examples

1. #Set the native-VLAN ID of bridge-map 1 to 100.

```
FS(config)#bridge-map 1
FS(config-bridge-map)#native-vlan 100
```

Verification

1. You can use the **show bridge-map** command to view the current native-vlan configuration.

Prompt Information

1. If you set native-VLAN ID of bridge-map 1 to 100, the system displays no prompt for successful configuration and you can use the new configuration to overwrite the existing one.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#bridge-map 1
FS(config-bridge-map)#native-vlan 100
```

2. If you specify an ID greater than 4094, the command fails.

Platform Description

This command is supported only in the bridging mode.

2.10 show bridge-map

Use this command to display information about the bridge-map.

show bridge-map *bridge-num* [**lan-ip**]

Parameter Description

Parameter	Description
bridge-map *bridge-num*	Bridge-map index.

Command Mode

Privileged EXEC mode, Global configuration mode, interface mode

Default Level

14

Usage Guide

By specifying the bridge-map index, you can display information about that bridge-map.

If you do not specify the bridge-map index, information about all bridge-maps will be displayed.

By specifying the lan-ip parameter, you can display the configuration of the IP address segment of the internal network in one-armed mode.

⚠ You must switch to a non-gateway mode to configure this command. For details about the command for switching to a non-gateway mode, see sys-mode.

Configuration Examples

1. #Display details of all bridge-maps.

```
FS# show bridge-map
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

BRIDGE MAP 1,STATE is DOWN
  Inside interface is NULL,Outside interface is NULL
  Working mode is null
  Native vlan is 1

BRIDGE MAP 2,STATE is DOWN
  Inside interface is NULL,Outside interface is NULL
  Working mode is null
  Native vlan is 1
```

Field description:

Field	Description
Inside interface	Inside interface composing the bridge
Outside interface	Outside interface composing the bridge
Working mode	Operating mode of the current bridge-map, including forward, sniffer, bypass and receive-only.
Native vlan	Native-VLAN ID of the current bridge-map

2. Display the configuration of the IP address segment of the internal network in one-armed mode.

```
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
```

Field description:

Field	Description
IP add	IP address of the internal network
mask add	Mask of the IP address segment of the internal network

Platform Description

This command is supported only in the bridging mode.

2.11 split

Use this command to split one 40GE port into four 10GE ports.

split slot *slot-num*

Use the **no** form of this command to restore the one 40GE port.

no split slot *slot-num*

Parameter Description

Parameter	Description
slot-num	Specifies the slot ID of the 40GE port to be split.

Defaults

By default, one 40GE port is in use.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1: This command is used to switch between one 40GE port and four 10GE port.

2: The configuration needs to be stored before taking effect.

Configuration Examples

1. # Switch the first 40GE port into four 10GE ports.

```
FS(config)#split slot 0
```

Verification

After the device restarts, run the **show running-config** command to display the configuration result.

After the device restarts, run the **show interface** command to generate four 10G ports. (slot 0 corresponds with TenGigabitEthernet 0/8 - 0/11 and slot 1 corresponds with TenGigabitEthernet 0/12 – 0/15)

Prompt Information

1. Configuration succeeds:

```
Please save the config, and reload system to take effect!
```

Common Errors

N/A

Platform Description

This command is only supported on EG3000XE and ACE5000E. There are two 40GE/10GE combo ports:

FortyGigabitEthernet 0/0 corresponds with TenGigabitEthernet 0/8, TenGigabitEthernet 0/9, TenGigabitEthernet 0/10 and TenGigabitEthernet 0/11;

FortyGigabitEthernet 0/1 corresponds with TenGigabitEthernet 0/12, TenGigabitEthernet 0/13, TenGigabitEthernet 0/14 and TenGigabitEthernet 0/15.

2.12 show mirror

Use this command to display all mirroring rules.

show mirror

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

1. #Display all mirroring rules.

```
master: 0
slave: 1(all) 2(rx) 3(tx)
```

Verification

N/A

Prompt Information

N/A

Common Errors

N/A

Platform Description

N/A.

2.13 show switch-info

Use this command to display Layer-2 and Layer-3 attributes and internal and external network attribute of the first 5 ports.

show switch-info

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

1. #Display Layer-2 and Layer-3 attributes and internal and external network attribute of the first 5 ports.

```
FS#show switch-info
PORT0     LAN6     0
PORT1     PORT1    1
PORT2     LAN4     1
PORT3     PORT3    1
PORT4     WAN2      1

FS#
```

Field Interpretation

Field	Description
PORT (First row)	Port number, corresponding with the five port numbers printed on the front panel.
PORT (Second row)	Layer-2 port
LAN	Layer-3 port, internal network port
WAN	Layer-3 port, external network port
The third row	Whether the switch between Layer-2 and Layer-3 is supported. “0” stands for not supporting while “1” for supporting.

Verification

N/A

Prompt Information

N/A

Common Errors

N/A

Platform Description

N/A

2.14 show sys-mode

Use this command to display information about system mode, and internal and external network attributes of interfaces.

show sys-mode

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, Global configuration mode, interface mode

Default Level 14

Usage Guide N/A

Configuration Examples

1. #Display system details.

```
FS# show sys-mode
System is gateway mode.
LAN: GigabitEthernet 0/0 GigabitEthernet 0/3
WAN: GigabitEthernet 0/1 GigabitEthernet 0/2 GigabitEthernet 0/4
```

Field description:

Field	Description
System	System mode
LAN	A list of interfaces with internal network attributes
WAN	A list of interfaces with external network attributes

Platform Description N/A

2.15 show write-db

Use this command to check whether the function of not storing logs in the local hard disk of the current device is enabled.

no write-db enable

write-db enable

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, interface mode

Default Level 14

Usage Guide N/A

Configuration 1. # Display whether the function of not storing logs in the local hard disk of the current device is enabled.

Examples

```
FS# show write-db
write-db enable: 0
```

Field description:

Field	Description
write-db enable	Whether the function of not storing logs in the local hard disk of the current device is enabled. “0” stands for not storing while “1” for storing.

Prompt Information

N/A

Platform Description

This command is only supported on high-end products, namely, EG2000X/XE/UE/G/GE, ACE3000E and ACE2000E.

2.16 specify interface

Use this command to configure the internal and external network attributes of the interface.

specify interface *interface-name* { **lan** | **wan** }

Use this command to remove the internal and external network attributes of the interface.

no specify interface *interface-name*

Parameter Description

Parameter	Description
interface *interface-name*	Specifies the interface name to be configured.
lan	Configures as an inside interface.
wan	Configures as an outside interface.

Defaults

Different device models have different default internal and external network attributes for network interfaces.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

In global configuration mode, use this command to configure the internal and external network attributes of the interface. Use the **no** form of this command to restore the interface attributes to the default values. Physical interfaces are supported.

The aggregate port has both internal and external network attributes, which are determined by the attributes of its member interfaces and cannot be manually switched.

Some sub-interfaces also have both internal and external network attributes: sub-interfaces of Ethernet ports and dialer ports. Their internal and external network attributes do not support manual configuration.

When being created, this type of sub-interface inherits internal and external network attributes from the main interface. The modified internal and external network attributes take effect after the main interface is restarted, and these attributes are then synchronized to the sub-interfaces.

To validate the modified internal and external network attributes, you need to save the configuration and restart the interface.

Configuration Examples

1. #Configure GigabitEthernet 0/0 as an inside interface.

```
FS(config)#specify interface GigabitEthernet 0/0 lan
```

Verification

1. You can use the **show sys-mode** command to view the internal and external network attributes of all network interfaces.

Prompt Information

1. The system displays no prompt for successful or repeated configuration.

2. If you configure the aggregate port as an outside interface, the system prompts that such configuration is not permitted.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#specify interface Aggregateport 0 wan
Converting interface attribute to wan is not supported on AP member.
```

Common Errors

1. Incorrect interface names are entered.

2.17 sys-mode

Use this command to set the system mode to gateway.

sys-mode gateway

Use this command to set the system mode to non-gateway (bridge)

no sys-mode gateway

Use this command to restore the default configuration.

default sys-mode gateway

Parameter Description

N/A

Defaults

The EG series and NBR series operate in gateway mode by default.

The ACE series and the MSC operate in bridge mode by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to specify the system operating in gateway mode or non-gateway mode. Save the configuration and restart the system to validate the configuration.

When the system operates in gateway mode, packet forwarding is based on the routing table and NAT translation is carried out. The network interface works as a layer-3 interface, and you can configure the IP address.

When the system operates in non-gateway mode, packets are forwarded according to the bridge-map and no

NAT translation is performed for packets. The network interface is a layer-2 interface, and you cannot configure the IP address.

Configuration Examples

1. #Set the system mode to non-gateway mode (bridge mode).

```
FS(config)# no sys-mode gateway
```

Verification

1. You can use the **show sys-mode** command to view the current system mode.

Prompt Information

1. If you modify the system mode, the system prompts that the modification takes effect after rebooting.

```
FS#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# no sys-mode gateway
System mode has changed, You must save config and reload the system.
```

Platform Description

N/A

2.18 vlan port

Use this command to add all layer-2 ports in the range of [min, max] to a VLAN and specifies whether a tag is carried.

vlan port *min max* **[tag]**

Use the **no** form of this command to remove all layer-2 ports from a VLAN.

no vlan port

Parameter Description

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.

Defaults

By default, all ports are in VLAN 4089.

Command Mode

Sub-interface mode

Default Level

14

Usage Guide

1. Encapsulate 802.1Q VLAN on a sub-interface before configuring this command.

2. This command only works on Layer-2 ports. Even if there are Layer-3 ports included in the port range, the command does not work on these Layer-3 ports.

3. Parameters: max >= min

Configuration

1. # Add Port 1 and Port 2 to VLAN 100 without tagging their packets.

Examples

```
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 configuration result.

```
…
interface GigabitEthernet 0/0.1
 encapsulation dot1Q 100
 vlan port 1 2
…
```

Prompt Information

1. Configuration succeeds. No prompts.

2. There is a Layer-3 port included in the range, and the configuration does not take effect on this port.

```
Warn: Port 3 is WAN port, this operation is invalid for this port!
```

3. No ports belong to the VLAN, so the **no vlan port** command does not take effect.

```
Warn: No ports belong to vlan 200, this operation is not valid!
```

4. The value of **max** is smaller than that of **min**.

```
Error: Max port number must greater than min port number!
```

5. 802.1Q VLAN is not encapsulated.

```
Error: No 802.1Q vlan is exist, this operation is not valid!
```

6. If the VLAN is not tagged initially, un the **no vlan port** command before modifying the tag.

```
Error: Vlan 200 is untagged, please execute 'no vlan port' before modifying the tag!
```

Common Errors

1: There is a Layer-3 port included in the range, and the configuration does not take effect on this port.

2: No ports belong to the VLAN, so the **no vlan port** command does not take effect.

3: The value of **max** is smaller than that of **min**.

4: 802.1Q VLAN is not encapsulated.

5: If the VLAN is not tagged initially, un the **no vlan port** command before modifying the tag.

Platform Description

N/A

2.19 xaui-mode

Use this command to configure 10GE port mode.

xaui-mode slot *slot-num*

Use the **no** form of this command to switches to four GE ports.

no xaui-mode slot *slot-num*

Parameter

Parameter	Description

Description

slot-num	Specifies the 10GE port, whose number is 2 or 3.

Defaults

The 10GE port mode is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to switch between four GE ports and one 10GE port.

This command needs to be saved and takes effect after restart of the device.

Configuration Examples

1. # Switch the first four GE ports into one 10GE port.

```
FS(config)#xaui-mode slot 2
```

Verification

1. After the device restarts, you can use the **show running-config** command to view configuration of the current 10GE port.

2. After the device restarts, run the **show interface** command, and then a 10GE port is generated. (Slot 2 corresponds with TenGigabitEthernet 0/2 and slot 3 corresponds with TenGigabitEthernet 0/3)

Prompt Information

1. Configuration succeeds:

```
Please save the config, and reload system to take effect!
```

Prompts starting with take effecterror warnings.

Platform Description

This command is only supported on EG2000X, EG2000XE, EG2000UE and ACE3000E.

When there are two GE/10GE ports: TenGigabitEthernet 0/2 corresponds with GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2 and GigabitEthernet 0/3, while TenGigabitEthernet 0/3 corresponds with GigabitEthernet 0/4, GigabitEthernet 0/5, GigabitEthernet 0/6 and GigabitEthernet 0/7.

3 DLDP Commands

3.1 clear dldp

Use this command to clear statistics about the times that DLDP is down or up at a specified monitoring point for renewing statistics.

clear dldp [**interface** *interface-name* [*ip-address*]]

Parameter Description

Parameter	Description
interface-name	Name of an Layer 3 interface
ip-address	IP address of a peer device

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

DLDP records statistics about the times that DLDP is down or up. You can use this command to clear statistics about the times that DLDP is down or up at a specified monitoring point and renew statistics. If an L3 interface or a device IP address is specified, statistics about the times that DLDP is down or up on the interface at one or all monitoring points will be cleared. If no L3 interface or IP address is specified, statistics about the times that DLDP is down or up at all monitoring points on all interfaces will be cleared.

Configuration Examples

The following example clears statistics about the times that DLDP is down or up at all monitoring points on all interfaces.

```
FS#clear dldp
```

The following example clears statistics about the times that DLDP is down or up at all monitoring points on the interface *vlan 1*.

```
FS#clear dldp interface vlan 1
```

The following example clears statistics about the times that DLDP is down or up about the peer device 10.83.132.1 on the interface *vlan 1*.

```
FS# clear dldp interface vlan 1 10.83.132.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.2 dldp

Use this command to configure DLDP detection.

Use the **no** form of this command to disable this function .

dldp *ip-address* [*next-hop-ip*] [**mac-address** mac-addr] [**interval** *tick* | **retry** *retry-num* | **resume** *resume-num*]

no dldp *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address of the peer device to be detected
next-hop-ip	Next-hop IP address specified when the device to be detected belongs to another different network
mac-address *mac-addr*	The bound MAC address. If a next hop exists, its MAC address is configured.
interval *tick*	Detection interval. The value range is from 1 to 6,000 in the unit of ticks, where 1 tick is equal to 10 milliseconds. The value must be an integral multiple of five.
retry *retry-num*	Number of retry times. The value range is from 1 to 3,600.
resume *resume-num*	Number of recovery times of the link to the peer device to be detected, indicating the number of consecutive packets received before a down link turns up. The value range is from 1 to 200.

Defaults

By default, *tick* is 100, indicating that the detection interval is 1 second.

The values of *retry-num* and *resume-num* are both 3.

Command Mode

Interface configuration mode

Usage Guide

You can use this command to enable DLDP detection to quickly detect Ethernet link faults.

DLDP detection detects multiple IP addresses on Layer 3 ports. If they respond no ICMP packets, they are considered down; if one of them recovers response, they are considered up.

Configuration Examples

```
The following example enables DLDP detection for the device 10.83.132.10.

FS#config

FS(config)#interface vlan 1

FS(config-if-VLAN 1)#ip address 10.83.132.1 255.255.255.0

FS(config-if-VLAN 1)#dldp 10.83.132.10


The following example enables DLDP detection for the device 10.83.132.10 in another different network segment.

FS#config

FS(config)#interface vlan 1

FS(config-if-VLAN 1)#ip address 10.83.132.1 255.255.255.0
FS(config-if-VLAN 1)#dldp 10.83.131.10 10.83.132.2
```

The following example disables DLDP detection for the device 10.83.132.10.

```
FS#config

FS(config)#interface vlan 1

FS(config-if-VLAN 1)#no dldp 10.83.132.10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.3 dldp interval

Use this command to set the DLDP detection interval.

Use the **no** form of this command to restore the default setting.

dldp interval *tick*

no dldp interval

Parameter Description

Parameter	Description
tick	Detection interval (in ticks), in the range from 5 to 6,000. The value must be a multiple of 5. (1tick = 10 milliseconds)

Defaults

The default is 10 ticks (100 ms).

Command Mode

Global configuration mode

Usage Guide

This command is used to set the DLDP detection interval.

If a device does not receive the reply packets from the peer device within the specific period (the time of this period is equal to that of the *detection packet retransmission interval* multiplied by the *retry count*), the device takes the L3 port as DOWN (though the physical link is up). Once the device receives the reply packets from the peer device, the device takes the L3 port as UP.

Configuration Examples

The following example sets the DLDP detection interval to 20 ticks.

```
FS#config

FS(config)#dldp interval 20
```

Related

Command	Description

Commands

N/A	N/A

Platform Description

N/A

3.4 dldp passive

Use this command to set DLDP to the passive mode.

Use the **no** form of this command to restore the default setting.

dldp passive

no dldp passive

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The default is the active mode.

Command Mode

Interface configuration mode

Usage Guide

If DLDP is enabled on devices at both ends of a link on a network and ICMP Echo packets are sent to each other for link detection, excessive packets exist between the two devices. If only one device sends ICMP Echo packets to the peer device on which the same detection parameters are configured, the peer device can detect whether the packets arrive in time and whether the link between them is normal. This method saves bandwidth and CPU resources.

You can set DLDP to the active mode for one device to initiate ICMP Echo packets, and set DLDP to the passive mode for the other device to passively receive the packets.

Configuration Examples

The following example sets DLDP to the passive mode.

```
FS#config

FS(config)#interface vlan 1

FS(config-if-VLAN 1)#ip address 10.83.132.1 255.255.255.0 //Set an IP address for vlan1.

FS(config-if-VLAN 1)#dldp passive
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.5 dldp resume

Use this command to set the DLDP recovery count.

Use the **no** form of this command to restore the default setting.

dldp resume *resume-num*

no dldp resume

Parameter Description

Parameter	Description
resume-num	Recovery count of the peer device link, in the range from 1 to 200. The parameter indicates the number of DLDP detection packets received consecutively from the peer device before the link status goes from DOWN to UP.

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide This command is used to set the DLDP recovery count.

Configuration Examples The following example sets the DLDP recovery count to 4.

```
FS#config
FS(config)#dldp resume 4
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 dldp retry

Use this command to set the DLDP retry count.

Use the **no** form of this command to restore the default setting.

dldp retry *retry-num*

no dldp retry

Parameter Description

Parameter	Description
retry-num	Retry count, in the range from 1 to 3,600

Defaults The default is 3.

Command Global configuration mode

Mode

Usage Guide This command is used to set the DLDP retry count.

Configuration Examples The following example sets the DLDP retry count to 4.

```
FS#config

FS(config)#dldp retry 4
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.7 show dldp

Use this command to display DLDP configuration information or statistics at various monitoring points.

show dldp [**interface** *interface-name*] [**statistic**]

Parameter Description

Parameter	Description
interface-name	Name of an L3 interface
statistic	Statistics

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide You can use this command with the keyword **statistics** to display statistics at all monitoring points on all interfaces or a specific Layer 3 interface. If a Layer 3 interface is specified, this command displays DLDP configuration and statistics at all monitoring points on the Layer 3 interface.

Configuration Examples The following example displays DLDP configuration information at all monitoring points on all interfaces.

```
FS#show dldp

Interface   Type          Ip           Next-hop      Interval   Retry   Resume   State

---------   -------   -----------   -----------   --------   -----   ------   ------

Vl2          Passive   192.168.6.3   192.168.2.2   10          5        3         Up

Vl3          Passive   192.168.7.3                  10          5        3         Up

Vl4          Passive   192.168.3.3   192.168.4.2   10          5        3         Up
```

The following example displays DLDP configuration information at all monitoring points on the Layer 3 interface *vlan 2*.

```
FS#show dldp intface vlan2

Interface   Type          Ip          Next-hop      Interval   Retry   Resume   State

---------   -------   -----------   -----------   --------   -----   ------   ------

Vl2          Passive   192.168.6.3   192.168.2.2   10          5        3         Up
```

The following example displays DLDP statistics at all monitoring points on all interfaces.

```
FS#show dldp statistic

Interface   Type          Ip          record-time   Up-count   Down-count

---------   -------   -----------   -----------   --------   ----------

Vl2          Passive   192.168.6.3   2h34m5s        10          9

Vl4          Passive   192.168.3.3   1d2h3m52s      10          9
```

The following example displays DLDP statistics at all monitoring points on the Layer 3 interface *vlan 2*.

```
FS#show dldp statistic interface vlan 2

Interface   Type          Ip          record-time   Up-count   Down-count

---------   -------   -----------   -----------   --------   ----------

Vl2          Passive   192.168.6.3   2h34m5s        10          9
```

Field	Description
record-time	Time length for recording the number of times that DLDP is up or down. The time is displayed in *y***d**h**m**s format: y: year d: day h: hour m: minute s: second Using the *Up-count* and *Down-count* parameters, you can check statistics about the number of times that DLDP is up or down within this time length.
Up-count	Number of times that DLDP is up at the specific monitoring point
Down-count	Number times that DLDP is down at the specific monitoring point

Related

Command	Description

Commands	N/A	N/A

Platform Description

N/A

4 PCAP Commands

4.1 packet capture file

Use this command to specify the name of the file to be saved.

packet capture file *filename* **[buffer-size** *buf-size***] [packet-num** *pkt-num***]**

Use this command to clear configurations for file saving and restore the configurations for outputting logs.

clear packet capture file

Parameter Description

Parameter	Description
filename	Name of the file to be saved
buf-size	Buffer size. The buffer size is 2 MB by default if this field is not specified. Packet capture automatically stops when the buffer is full.
pkt-num	Number of captured packets. Packet capture automatically stops when the number of captured packets reaches the specified value. The packet capture will continue by default unless otherwise specified.

Command Mode Privileged EXEC mode

Usage Guide The data of captured packets 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 as system logs. Only 30 packets can be output by default when no file name is set.

Configuration Example #Set the name of the file to be saved to **capture.pcap**, and set the number of captured packets to 100.

```
FS# packet capture file flash:capture.pcap packet-num 100
```

Verification Run the **show packet capture status** command to check whether the configuration succeeds.

4.2 packet capture point

Use this command to create capture points.

packet capture point *capture-point-name* **rule** *rule-name* **location {interface** *interface-name* | **vlan** *vlan-id* | **control-plane} {in | out | both}**

Use this command to clear capture points.

clear packet capture point *capture-point-name*

Parameter Description

Parameter	Description
capture-point-name	Name of a capture point
rule-name	Name of matching rule, which is defined by using the **packet capture rule** command
interface-name	Name of the interface for capturing packets
vlan-id	ID of the VLAN for capturing packet

control-plane	Packet capture on the control plane
in | out | both	Packet capture direction: inbound, outbound, or bidirectional.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Users can define multiple capture points (a maximum of 4 capture points are supported currently) at the same location as required, to match different capture rules or packet directions. The capture points can work simultaneously without affecting each other.

Configuration Example #Create a capture point for capturing CPU packets on the GI0/1 interface.

```
FS# packet capture point cap-1 rule tcp location interface gi0/1 both
```

Verification Run the **show packet capture status** command to check whether the configuration succeeds.

4.3 packet capture rule

Use this command to define a capture matching rule.

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*]

Use this command to clear a capture matching rule.

clear packet capture rule *rule-name*

Parameter Description

Parameter	Description
rule-name	Name of a matching rule
smac	Source MAC address
dmac	Destination MAC address
type | **ip** | **arp**	Layer-2 protocol type
sip	Source IP address
sip-mask	Source IP mask
dip	Destination IP address
dip-mask	Destination IP mask
protocol | **tcp** | **udp**	Layer-3 protocol type
sport	TCP/UDP source port
dport	TCP/UDP destination port

Command Mode Privileged EXEC mode

Usage Guide

1. Users can define multiple rules for packet capture and differentiate them by different names. After a rule is defined, the rule needs to be referenced by the capture point to actually take effect.
2. Before deleting the capture rule, all capture points referencing the rule need to be deleted.

Configuration Example

#Define a TCP capture matching rule.

```
FS# packet capture rule tcp etype ip protocol tcp
```

Verification

Run the **show packet capture status** command to check whether the configuration succeeds.

4.4 packet capture start

Use this command to start capturing packets.

packet capture start

Use this command to stop capturing packets.

packet capture stop

Parameter Description

Parameter	Description
start	Starts capturing packets.
stop	Stop capturing packets.

Command Mode

Privileged EXEC mode

Usage Guide

1. If the packet capture stop command is not entered after packet capture starts, the packet capture will automatically stop 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. Use the packet capture start command to capture packets at all capture points simultaneously.

Configuration Example

#Start capturing packet.

```
FS# packet capture start
```

Verification

Run the **show packet capture status** command to check whether the configuration succeeds.

4.5 show packet capture status

Use this command to display the packet capture information.

show packet capture status

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the packet capture information.

Configuration

N/A

Example

#Display the packet capture information as follows:

```
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/test.pcap
        buffer size: 2(MB)
        packets limit: 500
FS#
```

Field description:

Field	Description
Capture rule	Name of a capture rule
etype	Layer-2 protocol type
source MAC	Source MAC address
destination MAC	Destination MAC address
protocol	Layer-3 protocol type
source IP	Source IP address
destination IP	Destination IP address
source port	Source port
destination port	Destination port
Capture point	Name of a capture point
location	Location of a capture point
direction	Packet capture direction

buffer size	Buffer size
packets limit	Quantity limit of captured packets
filename	Name of an output file
status	Packet capture status
packets captured	Number of captured packets

N/A

5 PPPOE-CLIENT Commands

5.1 clear dialer

Use this command to clear statistics about the DDR dialer interface.

clear dialer

Parameter Description

Parameter	Description
N/A	N/A

Command Modes

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example clears statistics about the DDR dialer interface.

```
R1# clear dialer
```

Platform Description

N/A

5.2 clear pppoe tunnel

Use this command to clear all PPPoE tunnels.

clear pppoe tunnel

Parameter Description

Parameter	Description
N/A	N/A

Command Modes

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example clears all PPPoE tunnels.

```
R1# clear pppoe tunnel
```

Platform Description

N/A

5.3 dialer enable-timeout

Use this command to configure the timeout period for the ASDL line.

dialer enable-timeout *seconds*

Use the **no** form of this command to restore the default setting.

no dialer enable-timeout

Parameter Description

Parameter	**Description**
seconds	Configures the timeout period for the ASDL line in the unit of seconds.

Defaults The default is 15 seconds.

Command Modes Interface configuration mode

Usage Guide The timeout period for the ASDL line is the period from line disconnection or dial failure to the next dial.

Configuration Examples The following example configures the timeout period for the ASDL line to 20 seconds.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer enable-timeout 20
```

The following example restores the timeout period for the ASDL line to the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer enable-timeout
```

Platform Description N/A

5.4 dialer hold-queue

Use this command to configure a hold queue on a DDR dialer interface.

dialer hold-queue *packets* [**timeout** *seconds*]

Use the **no** form of this command to restore the default setting.

no dialer hold-queue [*packets* [**timeout** *seconds*]]

Parameter Description

Parameter	**Description**
packets	Sets the number of packets the queue can hold, in the range from 0 to 100.
timeout *seconds*	Sets the timeout period of the hold queue, in the unit of seconds. The default is 45 seconds.

Defaults This function is disabled by default.

Command Modes Interface configuration mode

Usage Guide

The device discards packets during negotiation after modem dialing. If this command is configured, packets in the hold queue will be saved on the device and sent once connection is created.

Configuration Examples

The following example sets the hold queue *packets* to 50.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer hold-queue 50
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer hold-queue
```

Platform Description

N/A

5.5 dialer idle-timeout

Use this command to specify the idle period for an ADSL line.

dialer idle-timeout *seconds*

Use the **no** form of this command to restore the default setting.

no dialer idle-timeout

Parameter Description

Parameter	Description
seconds	Sets the idle period for an ADSL line, in the unit of seconds.

Defaults

The default is 120 seconds.

Command Modes

Interface configuration mode

Usage Guide

This idle period refers to the period when no data traffic is transmitted in the ASDL line. The timer is reset when any message is received.

Configuration Examples

The following example sets the idle period to 60 seconds.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer idle-timeout 60
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer idle-timeout
```

Platform Description

N/A

5.6 dialer pool

Use this command to associate a dialer pool with a logical interface.

dialer pool *number*

Use the **no** form of this command to restore the default setting.

no dialer pool *number*

Parameter Description

Parameter	Description
number	Sets the ID of a dialer pool, in the range from 1 to 255.

Defaults

This function is disabled by default.

Command Modes

Interface configuration mode

Usage Guide

Advanced dialup requires association between a physical interface and a dialer interface through a dialer pool. First, add a physical interface to several dialer pools. Second, associate the logical interface with only one of the dialer pools. One physical interface may belong to multiple dialer pools but one logical interface is allowed to associate with one single dialer pool. The dialer interface selects an idle physical interface from the dialer pool randomly.

Configuration Examples

The following example associates dialer pool 1 with dialer interface1.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer pool 1
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer pool
```

Platform Description

N/A

5.7 dialer-group

Use this command to associate a dialer triggering rule with a DDR dialer interface.

dialer-group *group-number*

Use the **no** form of this command to restore the default setting.

no dialer-group

Parameter Description

Parameter	Description
group-number	The ID of a dialer triggering rule.

Defaults

This function is disabled by default.

Command Modes

Interface configuration mode

Usage Guide

The dialer triggering rule is configured by the **dialer-list** command. You should identify what packets can trigger dial before the association.

Configuration Examples

The following example associates a dialer triggering rule with DDR dialer interface 1.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer-group 1
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer-group
```

Platform Description

N/A

5.8 dialer-list

Use this command to define a dialer triggering rule.

dialer-list *dialer-group* **protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }

Use the **no** form of this command to restore the default setting.

no dialer-list *dialer-group* [**protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }]

Parameter Description

Parameter	Description
dialer-group	Sets the ID of a dialer triggering rule.
protocol *protocol-name*	Protocol name.
ip	Specifies the IP protocol to be used for defining a dialer triggering rule.
permit	Permits IP packets.
deny	Denies IP packets.
list	Specifies an access list to be used for defining a dialer triggering rule.
access-list-number	Sets the ID of an ACL list.

Defaults

This function is disabled by default.

Command Modes

Global configuration mode

Usage Guide

This configuration is mandatory to define one or more dialer triggering rules. Use the **dialer-group** command to apply these rules to specific dialer interfaces.

Configuration

The following example sets dialer triggering rule 1 to **ip**.

Examples

```
R1(config)# dialer-list 1 protocol ip permit
```

The following example restores the default setting.

```
R1(config)# no dialer-list 1
```

Platform Description

N/A

5.9 ip address

Use this command to enable the IP policy on an interface.

ip address { **negotiate |** *ip-addr subnet-mask* }

Use this command to disable the IP address acquisition mode.

no ip address

Parameter Description

Parameter	Description
negotiate	Enables an interface to acquire IP address through PPP negotiation.
ip-addr	The IP address of a specified interface.
subnet-mask	The mask of a specified interface.

Defaults

N/A

Command Modes

Interface configuration mode

Usage Guide

Use this command to configure the IP policy on a specified dialer interface. If PPP negotiation is enabled, the IP address is distributed by the server. If the IP address is specified manually, it takes effect only after negotiation with the server succeeds.

Configuration Examples

The following example sets the IP policy to PPP negotiation.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# ip address negotiate
```

The following example removes the IP policy configuration.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no ip address
```

Platform Description

N/A

5.10 ppp max-bad-auth

Use this command to setPPP authentication retry count.

ppp max-bad-auth *number*

Use the **no** form of this command to restore the default setting.

no ppp max-bad-auth

Parameter Description

Parameter	Description
number	Sets PPP authentication retry count, in the range from 1 to 255.

Defaults This function is disabled by default.

Command Modes Interface configuration mode

Usage Guide If *number* is set to 3, you can try twice after one failure t. If the last retry fails, The line will be reset.

Configuration Examples The following example Sets PPP authentication retry count to 3.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# ppp max-bad-auth 3
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no ppp max-bad-auth
```

Platform Description N/A

5.11 pppoe enable

Use this command to enable the PPPoE client function on the interface.

pppoe enable

Use the **no** form of this command to restore the default setting.

no pppoe enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Modes Interface configuration mode

Usage Guide Use this command on physical or aggregate WAN interfaces.

Configuration The following example enables the PPPoE client function on GigabitEthernet 0/5.

Examples

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# pppoe enable
```

The following example restores the default setting.

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# no pppoe enable
```

Platform Description

N/A

5.12 pppoe multi-dial enable

Use this command to enable the PPPoE client multi-dial function of the device. That is, multiple channels of PPPoE dialup can be configured on a physical port. If the function is disabled, only one channel of PPPoE dialup can be used on each physical port.

pppoe multi-dial enable

Use the **no** form of this command to disable the PPPoE client multi-dial function of the device.

no pppoe multi-dial enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The PPPoE client multi-dial function is disabled on the device by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to enable the PPPoE client multi-dial function and the function is disabled by default.

Configuration Examples

The following example enables the PPPoE client multi-dial function of the device in global configuration mode.

```
R1(config)# pppoe multi-dial enable
```

The following example disables the PPPoE client multi-dial function of the device.

```
R1(config)# no pppoe multi-dial enable
```

Verification

Run the **show running-config** command to check whether the configuration exists.

Prompts

N/A

Common Errors

N/A

Platform Description N/A

5.13 pppoe session mac-address

Use this command to configure the MAC address of a PPPoE session.

pppoe session mac-address *H.H.H*

Use the **no** form of this command to restore the default setting.

no pppoe session mac-address

Parameter Description

Parameter	Description
H.H.H	Configures the MAC address of a PPPoE session.

Defaults This function is disabled by default.

Command Modes Interface configuration mode

Usage Guide This configuration takes effect only on sub interfaces after the **pppoe enable** command is executed.

Configuration Examples The following example configures the MAC address of a PPPoE session on GigabitEthernet 0/5.1.

```
FS (config)# interface GigabitEthernet 0/5.1
FS(config-subif-GigabitEthernet 0/5.1)#pppoe enable
FS(config-subif-GigabitEthernet 0/5.1)#encapsulation dot1Q 1
FS(config-subif-GigabitEthernet 0/5.1)#pppoe sessiom mac-address 00d0.f822.33f3
```

The following example restores the default setting.

```
FS (config)# interface GigabitEthernet 0/5.1
FS(config-subif-GigabitEthernet 0/5.1)#no pppoe sessiom mac-address
```

Platform Description N/A

5.14 pppoe-client dial-pool-number

Use this command to add an Ethernet interface to a dialer pool and specifies the dial mode.

pppoe-client dial-pool-number *number* **no-ddr**

Use the **no** form of this command to restore the default setting.

no pppoe-client dial-pool-number *number*

Parameter Description

Parameter	Description

number	Sets the ID of a dialer pool.
no-ddr	Applies auto dial.

Defaults This function is disabled by default.

Command Modes Interface configuration mode

Usage Guide Use this command to add an Ethernet interface to a dialer pool, which is associated with the logical interface, In this way, the Ethernet interface and the logical interface are connected to perform dialing.

Configuration Examples The following example adds GigabitEthernet 0/5 to dialer pool 1.

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# pppoe-client dial-pool-number 1 no-ddr
```

The following example restores the default setting.

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# no pppoe-client dial-pool-number 1
```

Platform Description N/A

5.15 show pppoe

Use this command to display PPPoE information.

show pppoe { **ref** | **session** | **tunnel** }

Parameter Description

Parameter	Description
ref	Displays fast forwarding information about all PPPoE sessions.
session	Displays all PPPoE session information.
tunnel	Displays all PPPoE tunnel information.

Command Modes Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays fast forwarding information about all PPPoE sessions.

```
R1# show pppoe ref

 GigabitEthernet 0/6 Virtual-pppoe 2 dialer 1
  Protocol UP dialer-group 1 last_time 164235070 ms
  Ether Header: 00 60 4F 67 02 50 00 D0 F8 22 33 43 88 64
  PPPoE Header: 11 00 00 7F 00 50
```

```
   PPP Header     : 00 21
   DstMac 0060.4f67.0250, SrcMAC 00d0.f822.3343, SessionID 127
   Input Err : 0 MAC, 0 PPPoE Header
   Input Info: 0 Normal, 0 Drop, 345 Reserve, 0 Lost
   Output Err : 0 SessionState, 0 no ref, 0 length
   Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

 There is 1 pppoe session in System
```

The following example displays all PPPoE session information.

```
R1# show pppoe session
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is 00.60.4F.67.02.50
     Timer is running: 59750
```

The following example displays all PPPoE tunnel information.

```
R1# show pppoe tunnel
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is 00.60.4F.67.02.50
     Timer is running: 59003
```

Platform Description

N/A

6 PPPoE Server Commands

6.1 ac-cookie enable

Use this command to enable the AC cookie function in bba-group configuration mode.

ac-cookie enable

Use the **no** form of this command to disable the AC cookie function.

no ac-cookie enable

Use the **no** form of this command to restore the default configuration.

no ac-cookie enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The AC cookie function is disabled by default.

Command Mode

bba-group

Usage Guide

Use this command to enable the AC cookie function in bba-group PPPoE mode.

Configuration Example

#Enable AC cookie.

```
FS(config)# bba-group pppoe pppoe_server_group
FS(config-bba-group)# ac-cookie enable
```

Verification

Run the **show run** command to display the status of the AC cookie function.

6.2 bba-group pppoe

Use this command to configure a bba-group PPPoE dialup group in global configuration mode.

bba-group pppoe *bba-group-name*

Use the **no** form of this command to delete a bba-group.

no bba-group pppoe *bba-group-name*

Use this command to restore the default configuration.

default bba-group pppoe *bba-group-name*

Parameter Description

Parameter	Description
bba-group-name	Indicates the name of a bba-group.

Defaults

No bba-group is configured by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure a bba-group PPPoE group for dialup on the PPPoE server.

⚠ The name of a bba-group contains no more than 32 characters.

Configuration Example

#Configure a bba-group.

```
FS(config)# bba-group pppoe pppoe_server_group
```

Verification

Run the **show run** command to display the configuration result of the bba-group.

6.3 pppoe-server enable group

Use this command to enable the PPPoE server function on an interface.

pppoe-server enable group *group-name*

Use the **no** form of this command to disable the PPPoE server function.

no pppoe-server enable

Use this command to restore the default configuration.

default pppoe-server enable group

Parameter Description

Parameter	Description
group *group-name*	Indicates the bba-group dialup group associated with this interface.

Defaults

The PPPoE server function of an interface is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to enable the PPPoE server function in interface configuration mode for a L3 physical interface, L3 sub interface, or SVI. The name of a bba-group contains no more than 32 characters.

The PPPoE server function can be enabled on the SVI only for wireless products.

Configuration Example

#Enable the PPPoE server function on VLAN 3.

```
FS(config)# interface vlan 3
FS(config-if-VLAN 3)# pppoe-server enable group pppoe_server_group
```

Verification

Run the **show run** or **show interface** command to display the status of the PPPoE server function on the interface.

6.4 sessions local-mac limit

Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be received at a local MAC address of an interface associated with a bba-group.

sessions local-mac limit *limit-count*

Use the **no** form of this command to cancel the configuration.

no sessions local-mac limit

Use this command to restore the default configuration.

default sessions local-mac limit

Parameter Description

Parameter	Description
limit-count	Indicates the maximum number of sessions that can be received at a local MAC address. The value range is from 0 to 1,000.

Defaults

The maximum number of sessions that can be received at a local MAC address is 1,000 by default.

Command Mode

bba-group

Usage Guide

Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be received at a local MAC address.

Changing this parameter does not affect established sessions and the changed parameter takes effect only on the next established session.

If this parameter is set to **0**, the current interface does not allow PPPoE dialup.

Configuration Example

#Set the maximum number of sessions that can be received at the local MAC address associated with the pppoe_server_group to 50.

```
FS(config)# bba-group pppoe pppoe_server_group
FS(config-bba-group)# sessions local-mac limit 50
```

Verification

Run the **show run** command to display the maximum number of sessions that can be received at the local MAC address in a bba-group.

6.5 sessions max limit

Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be received by the current system.

sessions max limit *limit-count*

Use the **no** form of this command to cancel the configuration.

no sessions max limit

Use the **no** form of this command to restore the default configuration.

no sessions max limit

Parameter Description

Parameter	**Description**
limit-count	Indicates the maximum number of sessions that can be received by the current system. The value range is from 0 to 1,000.

Defaults The maximum number of sessions that can be received by the current system is 1,000 by default.

Command Mode bba-group

Usage Guide Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be received by the local system.

Changing this parameter does not affect established sessions and the changed parameter takes effect only on the next established session.

If this parameter is set to **0**, the current interface does not allow PPPoE dialup.

Configure this parameter in bba-group configuration mode to validate the value to all bba-groups. The value will be displayed under all bba-groups.

The latest configured value prevails.

Configuration Example #Set the maximum number of sessions that can be received by the current system to 500.

```
FS(config)# bba-group pppoe pppoe_server_group
FS(config-bba-group)# sessions max limit 500
```

Verification Run the **show run** command to display the configuration result of the bba-group.

6.6 sessions per-mac limit

Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be initiated from a peer MAC address of an interface associated with a bba-group.

sessions per-mac limit *limit-count*

Use the **no** form of this command to restore the default configuration.

no sessions per-mac limit

Use the **no** form of this command to restore the default configuration.

no sessions per-mac limit

Parameter Description

Parameter	**Description**
limit-count	Indicates the maximum number of sessions that can be initiated from a peer MAC address. The value range is from 0 to 500.

Defaults The maximum number of sessions that can be initiated from a peer MAC address is 100 by default.

Command Mode bba-group

Usage Guide Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be initiated from a peer MAC address.

Changing this parameter does not affect established sessions and the changed parameter takes effect only on the next established session.

If this parameter is set to **0**, the current interface does not allow PPPoE dialup.

Configuration Example #Set the maximum number of sessions that can be initiated from the peer MAC address associated with the pppoe_server_group to 50.

```
FS(config)# bba-group pppoe pppoe_server_group
FS(config-if)# sessions per-mac limit 50
```

Verification Run the **show run** command to display the configuration result of the bba-group.

6.7 virtual-template

Use this command to specify a virtual template interface to associate with the current bba-group PPPoE group.

virtual-template *interface-number*

Use the **no** form of this command to delete the virtual template.

no virtual-template *interface-number*

Use this command to restore the default configuration.

default virtual-template *interface-number*

Parameter Description

Parameter	Description
interface-number	Indicates the serial number of an interface.

Defaults No bba-group PPPoE group is associated with a virtual template interface by default.

Command Mode bba-group

Usage Guide Use this command to specify a virtual template interface to associate with the current bba-group PPPoE group.

Configuration Example #Specify virtual template interface 5 to associate with a bba-group PPPoE group.

```
FS(config)# bba-group pppoe pppoe_server_group
FS(config-bba-group)# virtual-template 5
```

Verification

Run the **show run** command to display the configuration result of the bba-group.

6.8 show pppoe-server

Use this command to display status information of a PPPoE server in privileged EXEC mode.

show pppoe-server { ref | session | tunnel } [session-id *sid* **]**

Parameter Description

Parameter	Description
ref	Displays all session information on the data plane.
session	Displays PPPoE session information.
tunnel	Displays PPPoE tunnel information.
session-id	Displays information about the specified session ID.
sid	Indicates the session ID.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

The session status of this command is consistent with the tunnel status.

Configuration Example

#Run the **show pppoe-server ref** command to display session information.

```
FS#show pppoe-server    ref
PPPOE Server ref current sessions count : 4
Sid: 2,In Intf:virtual-access 1,Out Intf:CAPWAP-Tunnel 1
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: C8-3A-35-C3-01-AC
             Input Info: 13 Normal, 0 Drop, 16 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

Sid: 3,In Intf:virtual-access 2,Out Intf:CAPWAP-Tunnel 1
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: D8-5D-4C-7F-10-0A
             Input Info: 2 Normal, 0 Drop, 13 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

Sid: 4,In Intf:virtual-access 0,Out Intf:CAPWAP-Tunnel 1
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: C8-3A-35-C0-B4-FC
             Input Info: 7 Normal, 0 Drop, 7 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost
```

Field description:

Field	Description
PPPOE Server ref current sessions count	Indicates the total number of sessions created on the data plane.
Sid	Indicates a session ID.
In Intf	Indicates a virtual interface for receiving packets

	corresponding to the current session.
Out Intf	Indicates a physical interface for transmitting packets of the current session.
LocalMAC	Indicates the MAC address of a local interface.
RemoteMAC	Indicates the MAC address of a remote interface.
Input Info	Indicates packet statistics of the inbound direction.
Normal	Indicates the number of packets that are normally received.
Drop	Indicates the number of abnormal packets that are received and need to be discarded.
Reserve	Indicates the number of packets that are sent to the control plane.
Lost	Indicates the number of packets that are received and then lost.
Output Info	Indicates packet statistics of the outbound direction.
Normal	Indicates the number of packets that are normally sent.
Drop	Indicates the number of abnormal packets that are sent and need to be discarded.
Reserve	Indicates the number of packets that are sent to the control plane.
Lost	Indicates the number of packets that are sent and then lost.

#Run the **show pppoe-server session** command to display session information.

```
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
```

Field description:

Field	**Description**
PPPOE Server current sessions count t	Indicates the total number of sessions created on the control plane.
Sid	Indicates a session ID.
State	STATE_SENT_IDLE idle STATE_SENT_PADI PADI sent STATE_RECEIVED_PADI PADI received STATE_SEND_PADO PADO sent STATE_RECEIVED_PADO PADO received

	STATE_SENT_PADR PADR sent STATE_RECEIVED_PADR PADR received STATE_SEND_PADS PADS sent STATE_SESSION session phase entered STATE_TERMINATED session terminated
intf	Indicates the interface of the current session.
External vid	Indicates an encapsulated VLAN ID.
Inner vid	Indicates an inner VLAN ID in the QINQ scenario. At present, QINQ termination is not supported, and therefore the value is always **0**.
PeerIP	Indicates an IP address allocated to the PPPoE client.
LocalMAC	Indicates the MAC address of a local interface.
RemoteMAC	Indicates the MAC address of a remote interface.
online time	Indicates the online duration of the current session.

7 PPP Commands

7.1 ppp accm

Use this command to configure the Asynchronous Control Character Map (ACCM) option for PPP negotiation.

ppp accm *value*

Use the **no** form of this command to restore the default setting.

no ppp accm

Parameter Description

Parameter	Description
value	Value of the ACCM option, in the range from 0 to 0xffffffff.

Command Mode

Interface configuration mode

Defaults

The default is 0x000A0000.

Default Level

14

Usage Guide

This command is used to configure the ACCM option involved in the PPP negotiation phase, in the range from 0 to 0xffffffff. The default is 0x000A0000.

Configuration Examples

The following example configures the ACCM option for PPP negotiation.

```
FS(config-if-Virtual-ppp 1)#ppp accm 0x0000000f
FS(config-if-Virtual-ppp 1)#
```

Verification

Run the **show running-config** command to display the value of the ACCM option configured on the current interface for PPP negotiation.

Note

N/A

Platform

N/A

7.2 ppp accounting

Use this command to configure the accounting mode of PPP.

ppp accounting { default | *list_name* **}**

Use the **no** form of this command to delete the accounting list of PPP.

no ppp accounting

Parameter

Parameter	Description

Description

default	Default accounting list
list_name	Name of the AAA accounting list

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

This command is used to configure the accounting mode of PPP. You can set the accounting mode to the default list or to the name of a specified accounting list. Before configuring this command, you need to enable the AAA module; otherwise, this command is invisible.

Configuration Examples

The following example configures the accounting mode of PPP.

```
FS(config-if-Virtual-ppp 1)#ppp accounting default
FS(config-if-Virtual-ppp 1)#ppp accounting acc_list
FS(config-if-Virtual-ppp 1)#
```

Verification

Run the **show running-config** command to display the name of the PPP accounting list configured on the current interface.

Note

N/A

Platform

N/A

7.3 ppp authentication

Use this command to configure the authentication mode of PPP.

ppp authentication { { **pap | chap** } [**callin** | { **chap | pap** } | **default** | *list_name*] }

Use the **no** form of this command to delete the authentication mode of PPP.

no ppp authentication { { **pap | chap** } [**callin** | { **chap** | **pap** } | **default** | *list_name*] }

Parameter Description

Parameter	Description
pap	Sets the authentication mode to PAP.
callin	Authenticates incoming request packets only.
chap	Sets the authentication mode to CHAP.
default	Uses the default authentication list, no matter whether PAP or CHAP authentication applies.
list_name	Configures the name of the authentication list.

Command Mode

Interface configuration mode

Default Level 14

Usage Guide This command is used to configure the authentication mode of PPP, which may be PAP or CHAP authentication.

Configuration Examples The following example configures the authentication mode of PPP.

```
FS(config-if-Virtual-ppp 1)#ppp authentication pap
FS(config-if-Virtual-ppp 1)#ppp authentication chap
FS(config-if-Virtual-ppp 1)#ppp authentication pap chap callin default
FS(config-if-Virtual-ppp 1)#ppp authentication pap chap test_list
FS(config-if-Virtual-ppp 1)#
```

Verification Run the **show running-config** command to display whether the authentication mode of PPP has been configured on the current interface.

Note N/A

Common Error N/A

Platform N/A

7.4 ppp authorization

Use this command to configure the authorization list of AAA authentication of PPP.

ppp authorization { **default** | *list_name* }

Use this command to delete the authorization list of AAA authentication of PPP

no ppp authorization

Parameter Description

Parameter	Description
default	Default authorization list of AAA authentication of PPP
list_name	Name of the specified authorization list of AAA authentication of PPP

Command Mode Interface configuration mode

Default Level 14

Usage Guide This command is used to configure the authorization list of AAA authentication of PPP. The authorization list of AAA authentication is used in the PPP authentication phase to perform AAA authentication. This command is visible only after the AAA module is enabled.

Configuration The following example sets the authorization list of PPP authentication on interface Virtual-PPP 1 to auth_list.

Examples

```
FS(config-if-Virtual-ppp 1)#ppp authorization default
FS(config-if-Virtual-ppp 1)#ppp authorization auth_list
FS(config-if-Virtual-ppp 1)#
```

Verification Run the **show running-config** command to display the authorization list of AAA authentication of PPP configured on the current interface.

Note N/A

Common Error N/A

Platform N/A

7.5 ppp chap

The following example configures the user name and password for CHAP authentication of PPP.

ppp chap hostname *name*

ppp chap password *password*

Use the **no** form of this command to delete the configured user name and password for CHAP authentication of PPP.

no ppp chap hostname

Parameter Description

Parameter	Description
name	User name for CHAP authentication
password	Password for CHAP authentication

Command Mode Interface configuration mode

Default Level 14

Usage Guide PPP negotiation is required for both VPDN and PPPOE dialing. The second phase of PPP negotiation is about user name and password authentication. This command is used to configure the user name and password for CHAP authentication.

Configuration Examples The following example configures the user name and password for CHAP authentication on interface Virtual-PPP 1.

```
FS(config-if-Virtual-ppp 1)#ppp chap hostname 111
FS(config-if-Virtual-ppp 1)#ppp chap password 111
FS(config-if-Virtual-ppp 1)#no ppp chap hostname
FS(config-if-Virtual-ppp 1)#
```

Verification Run the **show running-config** command to display the user name and password configured on the current interface for CHAP authentication.

Note N/A

Common Error N/A

Platform N/A

7.6 ppp ipcp dns

Use this command to configure the DNS option involved in the IPCP phase of PPP negotiation.

ppp ipcp dns { *A.B.C.D* [*A.B.C.D*] [**accept**] **|** **accept** | **request** | **reject** }

Use this command to delete the configured DNS option.

no ppp ipcp dns { *A.B.C.D* [*A.B.C.D*] [**accept**] | **accept** | **request** | **reject** }

Parameter Description

Parameter	Description
accept	Receives all non-0 DNS addresses.
request	Requests the DNS address from the peer server.
reject	Refuses to negotiate the DNS option with the peer end.
A.B.C.D	DNS address

Defaults The DNS option is not configured by default.

Command Mode Interface configuration mode

Default Level 14

Usage Guide This command is used to configure the DNS option involved in the IPCP negotiation phase.

Configuration Examples The following example configures the DNS option involved in the IPCP negotiation phase.

```
FS(config-if-Virtual-ppp 1)#ppp ipcp dns accept
FS(config-if-Virtual-ppp 1)#ppp ipcp dns reject
FS(config-if-Virtual-ppp 1)#ppp ipcp dns request
FS(config-if-Virtual-ppp 1)#ppp ipcp dns 1.1.1.1 2.2.2.2
FS(config-if-Virtual-ppp 1)#no ppp ipcp dns
FS(config-if-Virtual-ppp 1)#
```

Verification Run the **show running-config** command to display whether the DNS option has been configured on the current interface.

Note N/A

Common Error N/A

Platform N/A

7.7 ppp lcp mru negotiate

Use this command to configure the Maximum Receive Unit (MRU) option for PPP auto-negotiation.

ppp lcp mru negotiate

Use the no form of this command to remove the MRU configuration.

no ppp lcp mru

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Interface configuration mode

Default Level 14

Usage Guide The MRU option, as a common option involved in the PPP negotiation process, will be carried in packets from both ends during negotiation so as to determine the maximum size of packets to be transmitted on the entire link.

Configuration Examples The following example configures the MRU option for auto-negotiation on interface Virtual-ppp 1.

```
FS(config-if-Virtual-ppp 1)#ppp lcp mru negotiate
FS(config-if-Virtual-ppp 1)#
```

Verification 1. Run the **show running-config** command to display whether the MRU option has been configured on the current interface.

Note N/A

Common Error N/A

Platform N/A

7.8 ppp max-bad-auth

Use this command to specify the number of PPP authentication retries.

ppp max-bad-auth *number*

Use the **no** form of this command to restore the default setting.

no ppp max-bad-auth

Parameter Description

Parameter	Description
number	Number of PPP authentication retries, in the range from 1 to 255

Defaults The default is 1.

Command Mode Interface configuration mode

Default Level 14

Usage Guide The number of PPP authentication retries includes the first authentication; that is, if the number of PPP authentication retries is set to 3, twice authentication is still allowed following the failure of the first authentication. When the last authentication fails, the line is interrupted (or reset).

Configuration Examples The following example sets the number of PPP authentication retries on interface virtual-ppp1 to 3:

```
FS(config-if-Virtual-ppp 1)# ppp max-bad-auth 3
```

2The following example restores the number of PPP authentication retries to the default setting.

```
FS(config-if-Virtual-ppp 1)# no ppp max-bad-auth
```

Verification Run the **show running-config interface virtual-ppp** *1* command to display the configuration on the current interface.

Note N/A

Common Error N/A

Platform N/A

7.9 ppp negotiation-timeout

Use this command to specify the maximum PPP negotiation timeout period.

ppp negotiation-timeout *seconds*

Use the **no** form of this command to restore the default setting.

no ppp negotiation-timeout

Parameter Description

Parameter	Description
seconds	Maximum PPP negotiation timeout period, in the range from 10 to 65535 in the unit of seconds

Defaults The default is 20 seconds.

Command Mode Interface configuration mode

Default Level 14

Usage Guide If the maximum negotiation timeout period expires but PPP negotiation is not finished, the PPP negotiation is considered as having failed. The maximum PPP negotiation timeout period is 20s by default.

Configuration Examples The following example sets the maximum PPP negotiation timeout period on interface virtual-ppp1 to 200 seconds.

```
FS (config)# interface virtual-ppp 1
FS(config-if-Virtual-ppp 1)# ppp negotiation-timeout 200
```

The following example restores the maximum PPP negotiation timeout period to the default settings.

```
FS(config-if-Virtual-ppp 1)# no ppp negotiation-timeout
```

Verification Run the **show running-config interface virtual-ppp** *1* command to check the configuration on the current interface.

Note N/A

Common Error N/A

Platform N/A

7.10 ppp pap sent-username username password password

Use this command to configure the user name and password for PAP authentication of PPP.

ppp pap sent-username *username* **password** *password*

Use the **no** form of this command to delete the configured user name and password for PAP authentication of PPP.

no ppp pap sent-username

Parameter Description

Parameter	Description
username	User name for PAP authentication
password	Password for PAP authentication

Command Mode Interface configuration mode

Default Level 14

Usage Guide

PPP negotiation is required for both VPDN and PPPOE dialing. The second phase of PPP negotiation is about user name and password authentication. This command is used to configure the user name and password for PAP authentication.

Configuration Examples

The following example configures the user name and password for PAP authentication on interface Virtual-PPP 1.

```
FS(config-if-Virtual-ppp 1)#ppp pap sent-username 111 password 111
FS(config-if-Virtual-ppp 1)#no ppp pap sent-username
FS(config-if-Virtual-ppp 1)#
```

Verification

Run the **show running-config** command to display the user name and password configured on the current interface for PAP authentication.

Note

N/A

Common Error

N/A

Platform

N/A

8 Aggregate Port Commands

8.1 aggregateport load-balance

Use this command to configure a global load-balance algorithm for aggregate ports or a load-balance algorithm for an aggregate port . Use the **no** form of this command to return the default setting.

aggregateport load-balance { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst ip** | s **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** }

no aggregateport load-balance

Parameter Description

Parameter	Description
dst-mac	Load balance based on the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
src-mac	Load balance based on the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-ip	Load balance based on the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
dst-ip	Load balance based on the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
src-ip	Load balance based on the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
src-dst-mac	Load balance based on the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.
src-dst-ip-l4port	Load balance based on the source IP address, destination IP address, L4 source port number and L4 destination port number.
src- l4port	Load balance based on the L4 source port number.
dst- l4port	Load balance based on the L4 destination port number.
src-dst-l4port	Load balance based on the L4 source port number and L4 destination port number.
src-ip-src-l4port	Load balance based on the source IP address and the L4 source port number.
src-ip-dst-l4port	Load balance based on the source IP address and the L4 destination port number.
dst-ip-src-l4por	Load balance based on the destination IP address and the L4 source port number.

t	
dst-ip-dst-l4port	Load balance based on the destination IP address and the L4 destination port number.
src-ip-src-dst-l4port	Load balance based on the source IP address, L4 source port number and L4 destination port number.
dst-ip-src-dst-l4port	Load balance based on the destination IP address, L4 source port number and L4 destination port number.
src-dst-ip-src-l4port	Load balance based on the source IP address, the destination IP address and L4 source port number.
src-dst-ip-dst-l4port	Load balance based on the source IP address, the destination IP address and L4 destination port number.

Defaults The default load balance mode is **src-dst-mac** for the L2 AP port and **src-dst-ip** for the L3 AP port .
For the CB-card-loaded device supporting enhanced profile, load is balanced over AP according to packet type based the enhanced profile.

Command Mode Global configuration mode/Interface configuration mode

Usage Guide 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.

Configuration Examples The following example configures a load-balance algorithm globally based on the destination MAC address.

```
FS(config)# aggregateport load-balance dst-mac
```

Related Commands

Command	Description
show aggregateport load-balance	Displays aggregate port configuration.

Platform Description N/A

8.2 aggregateport member linktrap

Use this command to send LinkTrap to aggregate port members. Use the **no** form of this command to restore the default setting.

aggregateport member linktrap

no aggregateport member linktrap

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This function cannot be enabled by running the **snmp trap link-status** command in interface configuration mode.

Configuration Examples

The following example enables the LinkTrap function on the aggregate port members.

```
FS# configure terminal
FS(config)# aggregateport member linktrap
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.3 ap-interface wireport port-group

Use this command to configure member ports of the AP port via an access controller. Use the **no** form of this command to restore the default setting.

ap-interface wireport *port-number* **port-group** *ap-number*

no ap-interface wireport *port-number* **port-group**

Parameter Description

Parameter	Description
port-number	Wired port ofan access point
ap-number	AP port

Defaults

This function is disabled by default.

Command Mode

AP configuration mode/ AP group configuration mode

Usage Guide

You can configure this command on an access controller to add a wired port of an access point to an AP port. If this port is a member port of another AP port, the configuration does not take effect.

Configuration Examples

The following example adds port GigabitEthernet 0/1 of the access point to AggregatePort 1.

```
FS(config)#
FS(config)#ap-config 00d8.aabb.cc02
You are going to config AP(00d8.aabb.cc02), which is online now.
FS(config-ap)#ap-interface wireport 1 port-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.4 interfaces aggregateport

Use this command to create the aggregate port or enter interface configuration mode of the aggregate port. Use the **no** form of this command to restore the default setting.

interfaces aggregateport *ap-number*

no interfaces aggregateport *ap-number*

Parameter Description

Parameter	Description
ap-number	Aggregate port number.

Defaults The aggregate port is not created by default.

Command Mode Global configuration mode

Usage Guide If the aggregate port is created, this command is used to enter the interface configuration mode. Otherwise, this command is used to create the aggregate port and then enter its interface configuration mode.

Configuration Examples The following example creates AP 5 and enters its interface configuration mode.

```
FS# configure terminal
FS(config)# interfaces aggregateport 5
FS(config-if-Aggregateport 5)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.5 port-group

Use this command to assign a physical interface to be a member port of a static aggregate port. Use the **no** form of this command to restore the default setting.

port-group *port-group-number*

no port-group

Parameter Description

Parameter	Description
port-group-number	Member group ID of an aggregate port, the interface number of the aggregate port.

Defaults By default, the physical port does not belong to any aggregate port.

Command Mode Interface configuration mode.

Usage Guide All the members of an aggregate port belong to a VLAN or configured to be trunk ports. The ports belonging to different native VLANs cannot form an aggregate port.

Configuration Examples The following example specifies the Ethernet interface 1/3 as a member of the static AP 3.

```
FS(config)# interface gigabitethernet 1/3
FS(config-if-GigabitEthernet 1/3)# port-group 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.6 show aggregateport

Use this command to display the aggregate port configuration.

show aggregateport { [*aggregate-port-number*] **summary** | **load-balance** }

Parameter Description

Parameter	Description
aggregate-port-number	Number of the aggregate port.
load-balance	Displays the load-balance algorithm on the aggregate port.
summary	Displays the summary of the aggregate port.

Defaults N/A

Command Mode Any mode

Usage Guide If the aggregate port number is not specified, all the aggregate port information will be displayed.

Configuration Examples

```

N/A

```

Related Commands

Command	Description
aggregateport load-balance	Configures a load-balance algorithm of AP.

Platform N/A

Description

9 VLAN-TERMINAL Commands

9.1 show vid-info

Use this command to display the number of online clients with the same VID, and the IP addresses of the online clients with the VID.

show vid-info

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

14

Usage Guide

Use this command to display the number of online clients with the same VID, and the IP addresses of the online clients with the VID.

Configuration Example

#Display the number of online clients with the same VID, and the IP addresses of the online clients with the VID.

```
FS# show vid-info
vid            count           ip
100              1           192.168.1.2
102              2           192.168.1.10,192.168.1.12
```

9.2 show vlan-terminal

Use this command to display the VLAN-TERMINAL configuration information.

show vlan-terminal

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

14

Usage Guide

Use this command to display the current VLAN-TERMINAL configuration information.

Configuration Example

#Display current VLAN-TERMINAL configuration information.

```
FS# show vlan-terminal
vlan-terminal: enable
per-vlan:      20
Gi0/1:         1, 2, 60-80
Gi0/2:         4, 100-20
```

9.3 vlan-teminal per-vlan

Use this command to configure the maximum number of concurrent online clients of the same VLAN.

vlan-terminal per-vlan *num*

Parameter Description

Parameter	Description
num	Indicates the maximum number of concurrent online clients with the same VID. Once the number of concurrent online clients with the same VID reaches this value, no other client with the same VID can go online. The value range is from 1 to 1000.

Defaults

The maximum number of concurrent online clients with the same VID is 100 by default.

Command Mode

Global configuration mode

14

Usage Guide

Use this command to configure the maximum number of concurrent online clients with the same VID. The value range is from 1 to 1000.

Configuration Example

3. #Configure the maximum number of concurrent online clients with the same VID to 30.

```
FS#config
Enter configuration commands, one per line.   End with CNTL/Z.
FS(config)# vlan-terminal per-vlan 30
```

4. #Restore the maximum number of concurrent online clients with the same VID to the default value.

```
FS#config
Enter configuration commands, one per line.   End with CNTL/Z.
FS#no vlan-terminal per-vlan
```

Verification

Run the **show run** or **show vlan-terminal** command to display the maximum number of concurrent online clients belonging to the same VLAN.

9.4 vlan-terminal enable

Use this command to enable VLAN-TERMINAL

vlan-terminal enable

Use the **no** form of this command to disable VLAN-TERMINAL

no vlan-terminal enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

VLAN-TERMINAL is disabled by default.

Command Mode

Global configuration mode

14

Usage Guide

Configure this command to enable VLAN-TERMINAL.

Configuration Example

5. #Enable VLAN-TERMINAL on the device.

```
FS#config
FS(config)# vlan-terminal enable
```

6. #Disable VLAN-TERMINAL on the device.

```
FS#config
FS(config)#no vlan-terminal enable
```

Verification

1: Run the **show run** command to check whether VLAN-TERMINAL is enabled or disabled.

2: Run the **show vlan-terminal** command to display configurations.

9.5 vlan-terminal vlan-list

Use this command to configure the VID on a corresponding interface.

vlan-terminal vlan-list *vlan-list*

Parameter Description

Parameter	Description
vlan-list	Indicates a single VID or multiple VIDs separated by commas.

Defaults

N/A

Command Mode

Interface configuration mode

14

Usage Guide

Use this command to configure the VID on a corresponding interface.

Configuration Example

7. #Configure VIDs 2, 5, 40–80, and 100–120 on Interface 0/1

```
FS#config
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
```

8. #Delete configurations.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# interface gigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# no vlan-terminal vlan-list
```

Verification

Run the **show run** or **show vlan-terminal** command to display the maximum number of concurrent online clients belonging to the same VLAN.

1: The interface attribute is incorrect (only LAN interfaces are supported).

```
%Configuration fail: no lan interface.
```

2: The format is incorrect.

```
%Configuration fail: format error.
```

3: VIDs conflict.

```
%Configuration fail: the vid is conflict.
```

Chapter 6 IP Address & Application Commands

1 IP Address/Service Commands

1.1 gateway

Use this command to set the gateway address for the management port. Use the **no** form of this command to remove the setting.

gateway *address*

no gateway

Parameter Description

Parameter	Description
address	Sets the gateway address for the management port

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples

The following example sets the gateway address for the management port to 1.1.1.1.

```
FS(config)# interface mgmt 0
FS(config-if-Mgmt 0)# gateway 1.1.1.1
FS(config-if-Mgmt 0)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME.

1.2 ip-address

Use this command to configure the IP address of an interface. Use the **no** form of this command to restore the default setting.

ip address *ip-address network-mask* [**secondary**] | [**slave**]

no ip address [*ip-address network-mask* [**secondary**] | | [**slave**]

Parameter Description

Parameter	Description
ip-address	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.
network-mask	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.
secondary	Secondary IP address
slave	Slave IP address.

Defaults

No IP address is configured for the interface by default.

Command Mode

Interface configuration mode

Usage Guide

The equipment cannot receive and send IP packets before it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP).

The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value "1" are the network address. The IP address bits that correspond to value "0" are the host address. For example, the network mask of Class A IP address is "255.0.0.0". You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask.

The FSOS software supports multiple IP address for an interface, in which one is the primary IP address and others are the secondary/slave IP addresses. Theoretically, there is no limit for the number of secondary IP addresses. The primary IP address must be configured before the secondary IP addresses. The secondary IP address and the primary IP address must belong to the same network or different networks. Secondary IP addresses are often used in network construction. Typically, you can try to use secondary IP addresses in the following situations:

A network hasn't enough host addresses. At present, the LAN should be a class C network where 254 hosts can be configured. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the device should be connected to two networks and multiple IP addresses should be configured.

Many older networks are layer 2-based bridge networks that have not been divided into different subnets. Use of secondary IP addresses will make it very easy to upgrade this network to an IP layer-based routing network. The equipment configures an IP address for each subnet.

Two subnets of a network are separated by another network. You can create a subnet for the separated network, and connect the separated subnet by configuring a secondary IP address. One subnet cannot appear on two or more interfaces of a device.

Slave IP address is applied to the gateway cluster scenario. Only after the primary IP address is configured can the slave IP address be configured. Both slave and primary addresses are configured on an Layer 3 interface, backing up each other. In general, the master device adopts the primary IP address and the slave device uses the slave IP address. When the slave device becomes the master, its IP address becomes the primary IP address. When the master device turns into a slave, its IP address becomes the salve IP address,

In general, the layer-2 switch is configured a default gateway with the **ip default-gateway** command. Sometimes the layer-2 switch may be managed through the telnet, and the management IP and default gateway of the layer-2 switch needed to be modified. In this case, after configuring any one of the **ip address** and **ip default-gateway** command, the other cannot be configured any more due to the configuration change which causes failing to access this device through the network. So you need to use the keyword **gateway** in the **ip address** command to modify both the management IP and default gateway. The keyword **gateway** is not in the output of **show running config**, but in the output of **ip default-gate** command.

Configuration Examples

The following example configures the primary IP address and the network mask as 10.10.10.1 and 255.255.255.0 respectively .

```
FS(config-if)# ip address 10.10.10.1 255.255.255.0
```

The following example configures the default gateway address as 10.10.10.254.

```
FS(config-if)# ip address 10.10.10.1 255.255.255.0 gateway 10.10.10.254
```

The following example configures the master and slave IP addresses as 10.10.10.1/24 and 10.10.20.1/24 respectively.

```
FS(config)# interface gigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0
FS(config-if-GigabitEthernet 0/1)# ip address 10.10.20.1 255.255.255.0 slave
```

Related Commands

Command	Description
show interface	Displays detailed information of the interface.

Platform Description

N/A

1.3 ip address negotiate

Use this command to configure an IP address for the interface through PPP negotiation. Use the **no** form of this command to restore the setting.

ip address negotiate

no ip address negotiate

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Only the PPP interface of the router supports IP address configuration through PPP negotiation. After the interface is configured with the **ip address negotiate** command, the peer end should be configured with the **peer default ip address** command.

Configuration Examples

The following example obtains an IP address for the interface through PPP negotiation.

```
FS(config)# interface dialer 1
FS(onfig-if-dialer 1)# ip address negotiate
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.4 ip address-pool local

Use this command to enable the IP address pool function. Use the **no** form of this command to disable this function.

ip address-pool local

no ip address-pool local

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide This function is enabled by default. PPP users can allocate an IP address to the peer end from the IP address pool configured. If you can use the **no ip address-pool local** command to disable this function and clear all configured IP address pools.

Configuration Examples The following example enables the IP address pool function.

```
FS(config)# ip address-pool local
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.5 ip broadcast-addresss

Use this command to define a broadcast address for an interface in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip broadcast-addresss *ip-address*

no ip broadcast-addresss

Parameter Description

Parameter	Description
ip-address	Broadcast address of IP network

Defaults The default IP broadcast address is 255.255.255.255.

Command Mode Interface configuration mode.

Usage Guide At present, the destination address of IP broadcast packet is all "1", represented as 255.255.255.255. The FSOS software can generate broadcast packets with other IP addresses through definition, and can receive both all "1" and the broadcast packets defined by itself.

Configuration Examples The following example sets the destination address of IP broadcast packets generated by this interface to 0.0.0.0.

```
FS(config)# interface gigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ip broadcast-address    0.0.0.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.6 ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip directed-broadcast [*access-list-number*]

no ip directed-broadcast

Parameter Description

Parameter	Description
access-list-number	(Optional) Access list number, in the range from 1 to 199 and from 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all "1"), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets.

You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast.

If the **no ip directed-broadcast** command is configured on an interface, FSOS will discard the directed broadcast packets received from the directly connected network.

Configuration Examples

The following example enables forwarding of directed broadcast packet on the fastEthernet 0/1 port of a device.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# ip directed-broadcast
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.7 ip icmp error-interval

Use this command to set the rate to send the ICMP destination unreachable packets triggered by DF in the IP header. Use the **no** form of this command to restore the default setting.

ip icmp error-interval DF *milliseconds [bucket-size]*

no ip icmp error-interval DF *milliseconds* [*bucket-size*]

Use this command to set the rate to send other ICMP error packets. Use the **no** form of this command to restore the default setting.

ip icmp error-interval *milliseconds [bucket-size]*

no ip icmp error-interval *milliseconds* [*bucket-siz*]

Parameter Description

Parameter	Description
milliseconds	The refresh period of the token bucket, in the range from 0 to 2147483647 in the unit of milliseconds. 0 indicates no limit on the rate to send ICMP error packets. The default is 100.
bucket-size	The number of tokens in the bucket, in the range is from 1 to 200. The default is 10.

Defaults

The default rate is 10 packets per 100 millisecond.

Command Mode

Global configuration mode.

Usage Guide

To prevent DoS attack, the token bucket algorithm is adopted to limit the rate to send ICMP error packets.

If IP packets need to be fragmented while the DF is set to 1, the device sends ICMP destination unreachable packets numbered 4 to the source IP address for path MTU discovery. Rate limits on ICMP destination unreachable packets and other error packets are needed to prevent path MTU discovery failure.

It is recommended to set the refresh period to an integral multiple of 10 milliseconds. If the refresh period is not an integral multiple of 10 milliseconds, it is adjusted automatically. For example, 1 per 5 milliseconds is adjusted to 2 per 10 milliseconds; 3 per 15 milliseconds is adjusted to 2 per 10 milliseconds.

Configuration Examples

The following example sets the rate to send the ICMP destination unreachable packets triggered by DF in the IP header to 100 per second.

```
FS(config)# ip icmp error-interval DF 1000 100
```

The following example sets the rate to send other ICMP error packets to 10 per second.

```
FS(config)# ip icmp error-interval 1000 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.8 ip local pool

Use this command to create an IP address pool. Use the **no** form of this command to remove the setting.

ip local pool *pool-name low-ip-address* [*high-ip-address*]

no ip local pool *pool-name* [*low-ip-address* [*high-ip-address*]]

Parameter Description

Parameter	Description
pool-name	Specifies the address pool name. The default name is **default**.
low-ip-address	The start IP address in the address pool.
high-ip-address	(Optional) The end IP address in the address pool.

Defaults

No IP address pool is configured by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to create one or multiple IP address pools for PPP to allocate addresses to users.

Configuration Examples

The following example creates an IP address pool named quark ranging from 172.16.23.0 to 172.16.23.255.

```
FS(config)#ip local pool quark 172.16.23.0 172.16.23.255
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.9 ip mask-reply

Use this command to configure the FSOS software to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. Use the **no** form of this command to restore the default setting.

ip mask-reply

no ip mask-reply

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command mode

Interface configuration mode.

Usage Guide

Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.

Configuration Examples

The following example sets the FastEthernet 0/1 interface of a device to respond the ICMP mask request message.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# ip mask-reply
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.10 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. Use the **no** form of this command is restore the default setting.

ip mtu *bytes*

no ip mtu

Parameter Description

Parameter	Description
bytes	Maximum transmission unit of IP packet , in the range from 68 to 1500 bytes

Defaults It is the same as the value configured in the interface command **mtu** by default.

Command Mode Interface configuration mode.

Usage Guide If an IP packet is larger than the IP MTU, the FSOS software will split this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface.

If the interface configuration command **mtu** is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.

Configuration Examples The following iexample sets the IP MTU value of the fastEthernet 0/1 interface to 512 bytes.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# ip mtu 512
```

Related Commands

Command	Description
mtu	Sets the MTU value of an interface.

Platform Description N/A

1.11 ip redirects

Use this command to allow the FSOS software to send an ICMP redirection message in the interface configuration mode. Use the **no** form of this command to disable this function.

ip redirects

no ip redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path.

Configuration Examples

The following example disables ICMP redirection for the fastEthernet 0/1 interface.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# no ip redirects
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.12 ip source-route

Use this command to allow the FSOS software to process an IP packet with source route information in global configuration mode. Use the **no** form of this command to disable this function.

ip source-route

no ip source-route

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Global configuration mode.

Usage Guide

FSOS supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded.

Configuration Examples

The following example disables the IP source route.

```
FS(config)# no ip source-route
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.13 ip ttl

Use this command to set the TTL value of the unicast packet. Use the **no** form of this command to restore the default setting.

ip ttl *value*

no ip ttl

Parameter Description

Parameter	Description
value	Sets the TTL value of the unicast packet, in the range from 0 to 255.

Defaults

The default is 64.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the TTL value of the unicast packet to 100.

```
FS(config)# ip ttl 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.14 ip unnumbered

This command is used to configure unnumbered interfaces. After an interface is set to an unnumbered interface, IP can be run on the interface and packets can be sent or received on the interface. Use the **no** form of this command to restore the default setting.

ip unnumbered *interface-type interface-number*

no ip unnumbered

Parameter Description

Parameter	Description
interface-type	Type of the associated interface
interface-number	No. of the associated interface

Defaults

No unnumbered interface is configured by default.

Command mode

Interface configuration mode

Usage Guide

An unnumbered interface indicates that IP is enabled on the interface but no IP address is allocated for the interface. An unnumbered interface must associate with an interface with an IP address. The source IP address of the IP packets generated on an unnumbered interface is the IP address of the associated interface. In addition, the routing protocol process determines whether to send route update packets to the unnumbered interface according to the IP address of the associated interface. Pay attention to the following when using an unnumbered interface:

An Ethernet interface cannot be set to an unnumbered interface.

When SLIP, HDLC, PPP, LAPB, and Frame-relay are encapsulated on a serial port, the port can be set to an unnumbered interface. When a frame relay is encapsulated, only a point-to-point subinterface can be set to an unnumbered interface. In the case of X.25 encapsulation, unnumbered interface is not allowed.

The **ping** command cannot be used to check whether an unnumbered interface is working properly because the interface does not have an IP address. The status of an unnumbered interface can be remotely monitored over SNMP.
The network cannot be enabled using an unnumbered interface.

Configuration Examples

The following example configures the local interface as an unnumbered interface and sets the associated interfacet to FastEthernet 0/1 (an IP address is configured for the interface).

```
FS(config-if)# ip unnumbered fastEthernet 0/1
```

Related Commands

Command	Description
show interface	Displays the detailed information about the interface.

Platform Description

N/A

1.15 ip unreachables

Use this command to allow the FSOS software to generate ICMP destination unreachable messages. Use the **no** form of this command to disable this function.

ip unreachables

no ip unreachables

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode.

Usage Guide

FSOS software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upper protocol of this message.

FSOS software will send ICMP host unreachable message to source data if it can not forward a message due to no routing.

This command influences all ICMP destination unreachable messages.

Configuration Examples

The following example disables sending ICMP destination unreachable message on FastEthernet 0/1.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# no ip unreachables
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.16 peer default ip address

Use this command to allocate an IP address to the peer end through PPP negotiation. Use the **no** form of this command to restore the default setting.

peer default ip address { *ip-address* | **pool** [*pool-name*] }

no peer default ip address

Parameter Description

Parameter	Description
ip-address	Allocates an IP address to the peer end.
pool-name	(Optional) Specifies the address pool name. If not specified, the default address pool is used.

Defaults

No IP address is allocated to the peer end through PPP negotiaon by default.

Command Mode

Interface configuration mode.

Usage Guide

If the local end is configured with an IP address while the peer end not, you can enable the local end to allocate an IP address to the peer end by configuring the **ip address negotiate** command on the peer end and the **peer default ip address** on the local end.

This command is configured on PPP interface supporting encapsulation PPP or SLIP.

The **peer default ip address pool** command is used to allocate an IP address to the peer end from the address pool, configured by using the **ip local poo**l command.

The **peer default ip address** *ip-address* command is used to specify an IP address for the peer end. This command cannot be configured on virtual template interfaces and asyn interfaces.

Configuration Examples

The following example enables interface dialer 1 to allocate IP address 10.0.0.1 to the peer end.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# peer default ip address 10.0.0.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.17 show ip interface

Use this command to display the IP status information of an interface.

show ip interface [*interface-type interface-number* | **brief**]

Parameter Description

Parameter	Description
interface-type	Specifies interface type.
interface-number	Specifies interface number.
brief	Displays the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

When an interface is available, FSOS will create a direct route in the routing table. The interface is available in that the FSOS software can receive and send packets through this interface. If the interface changes from available status to unavailable status, the FSOS software removes the appropriate direct route from the routing table.

If the interface is unavailable, for example, two-way communication is allowed, the line protocol status will be shown as "UP". If only the physical line is available, the interface status will be shown as "UP".

The results shown may vary with the interface type, because some contents are the interface-specific options

Configuration Examples

The following exmaple displays the output of the **show ip interface brirf command**.

```
FS#show ip interface brief
Interface IP-Address(Pri) IP-Address(Sec) Status Protocol
GigabitEthernet 0/10 2.2.2.2/24 3.3.3.3/24 down down
GigabitEthernet 0/11 no address no address down down
VLAN 1 1.1.1.1/24 no address down down
```

Description of fields:

Field	Description
Status	Link status of an interface. The value can be **up**, **down**, or **administratively down**.
Protocol	IPv4 protocol status of an interface.

The following example displays the output of the **show ip interface vlan** command.

```
SwitchA#show ip interface vlan 1
VLAN 1
 IP interface state is: DOWN
 IP interface type is: BROADCAST
 IP interface MTU is: 1500
 IP address is:
 1.1.1.1/24 (primary)
 IP address negotiate is: OFF
 Forward direct-broadcast is: OFF
 ICMP mask reply is: ON
 Send ICMP redirect is: ON
 Send ICMP unreachabled is: ON
 DHCP relay is: OFF
 Fast switch is: ON
 Help address is:
 Proxy ARP is: OFF
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
```

Description of fields in the results:

Field	Description
IP interface state is:	The network interface is available, and both its interface hardware status and line protocol status are "UP".
IP interface type is:	Show the interface type, such as broadcast, point-to-point, etc.
IP interface MTU is:	Show the MTU value of the interface.
IP address is:	Show the IP address and mask of the interface.
IP address negotiate is:	Show whether the IP address is obtained through negotiation.
Forward direct-broadcast is:	Show whether the directed broadcast is forwarded.
ICMP mask reply is:	Show whether an ICMP mask response message is sent.
Send ICMP redirect is:	Show whether an ICMP redirection message is sent.
Send ICMP unreachabled is:	Show whether an ICMP unreachable message is sent.
DHCP relay is:	Show whether the DHCP relay is enabled.
Fast switch is:	Show whether the IP fash switching function is enabled.
Route horizontal-split is:	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Show the helper IP address.
Proxy ARP is:	Show whether the agent ARP is enabled.
ARP packet input number: Request packet:	Show the total number of ARP packets received on the interface, including:

Reply packet: Unknown packet:	ARP request packet ARP reply packet Unknown packet
TTL invalid packet number:	Show the TTL invalid packet number
ICMP packet input number: Echo request: Echo reply: Unreachable: Source quench: Routing redirect:	Show the total number of ICMP packets received on the interface, including: Echo request packet Echo reply packet Unreachable packet Source quench packet Routing redirection packet
Outgoing access list is	Show whether an outgoing access list has been configured for an interface.
Inbound access list is	Show whether an incoming access list has been configured for an interface.

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A.

1.18 show ip packet queue

Use this command to display the statistics of IP packet queues.

show ip packet queue

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

The following example displays the statistics of IP packet queues.

```
FS#show ip packet queue
Receive 31925 packets(fragment=0):
  IP packet receive queue: length 0, max 1542, overflow 0.
  Receive 13 ICMP echo packets, 25 ICMP reply packets .
  Discards:
    Failed to alloc skb: 0.
    Receive queue overflow: 0.
    Unknow protocol drops: 0.
    ICMP rcv drops: 0. for skb check fail.
    ICMP rcv drops: 0. for skb is broadcast.
Sent packets:
  Success: 15644
  Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets.
  It records 187 us as max time in ICMP reply process.
Failed to alloc efbuf: 0
  Dropped by EFMP: 0
  NoRoutes: 887
  Get vrf fails: 0
  Cannot assigned address drops: 0
  Failed to encapsulate ethernet head: 0
ICMP error queue: length 0, max 1542, overflow 0.
```

Field	Description
IP packet receive queue	Statistics of received packets
Discards	Statistics of discarded packets
Sent packets	Statistics of sent packets
ICMP error queue	Statistics of ICMP error packets

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.19 show ip packet statistics

Use this command to display the statistics of IP packets.

show ip packet statistics [**total** | *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name
total	Displays the total statistics of all interfaces.

Defaults N/A.

Command Mode Privileged EXEC mode.

Usage Guide N/A.

Configuration The following example displays the output of this command.

Examples

```
R1#show ip packet statistics
Total
  Received 113962 packets, 11948991 bytes
    Unicast:90962,Multicast:5232,Broadcast:17768
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 34917 packets, 1863146 bytes
    Unicast:30678,Multicast:4239,Broadcast:0
GigabitEthernet 0/1
  Received 6715 packets, 416587 bytes
    Unicast:2482,Multicast:4233,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 6720 packets, 417096 bytes
    Unicast:2481,Multicast:4239,Broadcast:0
Loopback 0
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
Tunnel 1
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 21584 packets, 1122848 bytes
Unicast:21584,Multicast:0,Broadcast:0
```

Related Commands

Command	Description
ip default-gateway	Configures the default gateway, which is only supported on the Layer 2 switch.

Platform Description

N/A

1.20 show ip pool

Use this command to display the IP address pool.

show ip pool [*pool-name*]

Parameter Description

Parameter	Description
pool-name	Specifies the IP address pool.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays all IP address ranges.

```
FS# show ip pool
FS(config)#show ip pool
Pool                    Begin                End                         Free      In use
default               1.1.1.1              1.1.1.1                         1             0
pool1                  2.2.2.2              2.2.2.254                   253             0
pool2                  3.1.1.1              3.2.1.1                   65537             0
pool3                  192.168.1.1          192.168.1.254
```

Field	Description
Pool	Address pool name
Begin	The start IP address of the address pool
Free	The number of free IP addresses in the address pool
In use	The number of IP addresses in use in the address pool

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.21 show ip raw-socket

Use this command to display IPv4 raw sockets.

show ip raw-socket [*num*]

Parameter Description

Parameter	Description
num	Protocol.

Defaults N/A.

Command Mode

Priviledged EXEC mode.

Usage Guide

N/A.

Configuration Examples

The following example displays all IPv4 raw sockets.

```
FS# show ip raw-socket
Number Protocol Process name
1         ICMP        dhcp.elf
2         ICMP        vrrp.elf
3         IGMP        igmp.elf
4         VRRP        vrrp.elf
Total: 4
```

Field Description

Field	Description
Number	Number
Protocol	Protocol
Process name	Process name
Total	Total number

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.22 show ip sockets

Use this command to display all IPv4 sockets.

show ip sockets

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

The following displays all IPv4 sockets.

```
FS# show ip sockets
Number Process name        Type        Protocol LocalIP:Port    ForeignIP:Port                    State
```

```
1         dhcp.elf              RAW          ICMP         0.0.0.0:1          0.0.0.0:0                              *
2         vrrp.elf              RAW          ICMP         0.0.0.0:1          0.0.0.0:0                              *
3         igmp.elf              RAW          IGMP         0.0.0.0:2          0.0.0.0:0                              *
4         vrrp.elf              RAW          VRRP         0.0.0.0:112        0.0.0.0:0                              *
5         dhcpc.elf             DGRAM        UDP          0.0.0.0:68         0.0.0.0:0                              *
6         fs-snmpd              DGRAM        UDP          0.0.0.0:161        0.0.0.0:0                              *
7         wbav2                 DGRAM        UDP          0.0.0.0:2000       0.0.0.0:0                              *
8         vrrp_plus.elf         DGRAM        UDP          0.0.0.0:3333       0.0.0.0:0                              *
9         mpls.elf              DGRAM        UDP          0.0.0.0:3503       0.0.0.0:0                              *
10        rds_other_th          DGRAM        UDP          0.0.0.0:3799       0.0.0.0:0                              *
11        fs-snmpd              DGRAM        UDP          0.0.0.0:14800 0.0.0.0:0                                   *
12        fs-sshd               STREAM       TCP          0.0.0.0:22         0.0.0.0:0                              LISTEN
13        fs-telnetd            STREAM       TCP          0.0.0.0:23         0.0.0.0:0                              LISTEN
14        wbard                 STREAM       TCP          0.0.0.0:4389       0.0.0.0:0                              LISTEN
15        wbard                 STREAM       TCP          0.0.0.0:7165       0.0.0.0:0                              LISTEN
Total: 15
```

Field Description

Field	Description
Number	Serial number.
Process name	Process name.
Type	Socket type, including the following types: RAW: raw sockets DGRAM: datagram type STREAM: stream type.
Protocol	Protocol.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	Peer IP address and port.
State	State. This field is for only TCP sockets.
Total	The total number of sockets.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.23 show ip udp

Use this command to display IPv4 UDP sockets.

show ip udp [**local-port** *num*]

Use this command to display IPv4 UDP socket statistics.

show ip udp statistics

Parameter Description

Parameter	Description
local-port *num*	Local port number

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

The following example displays all IPv4 UDP sockets.

```
FS# show ip udp
Number Local Address        Peer Address        Process name
1      0.0.0.0:68           0.0.0.0:0           dhcpc.elf
2      0.0.0.0:161          0.0.0.0:0           fs-snmpd
3      0.0.0.0:2000         0.0.0.0:0           wbav2
4      0.0.0.0:3333         0.0.0.0:0           vrrp_plus.elf
5      0.0.0.0:3503         0.0.0.0:0           mpls.elf
6      0.0.0.0:3799         0.0.0.0:0           rds_other_th
7      0.0.0.0:14800        0.0.0.0:0           fs-snmpd
```

Field Description

Field	Description
Number	Number.
Local Address	Local IP address and port.
Peer Address	Peer IP address and port.
Process name	Process name.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2 ARP Commands

2.1 arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. Use the **no** form of this command to restore the default setting.

arp *ip-address MAC-address type* [**description** *string*]

no arp *ip-address*

Parameter Description

Parameter	Description
ip-address	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
MAC-address	48-bit data link layer address
type	ARP encapsulation type. The keyword is arpa for the Ethernet interface.
string	Description information of a static ARP, containing a maximum of 32 characters.

Defaults

There is no static mapping record in the ARP cache table by default.

Command Mode

Global configuration mode.

Usage Guide

FSOS finds the 48-bit MAC address according to the 32-bit IP address using the ARP cache table.

Since most hosts support dynamic ARP resolution, usually static ARP mapping is not necessary. The **clear arp-cache** command can be used to delete the ARP mapping that is learned dynamically.

Configuration Examples

The following example sets an ARP static mapping record for a host in the Ethernet.

```
FS(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

The following example adds description information, ABC.

```
FS(config)# arp 1.1.1.1 4e54.3800.0002 arpa description ABC
```

Related Commands

Command	Description
clear arp-cache	Clears the ARP cache table

Platform Description

N/A

2.2 arp any-ip

Use this command to enable any IP ARP function.

Use the **no** form of this command to restore the default setting.

arp any-ip

no arp any-ip

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

You should modify the configuration to access the network in the following two cases:

The client IP address is in the network segment configured on an interface connected directly with the device, but the gateway IP address is not the IP address configured for the directly connected interface.

The client IP address is not in the network segment configured on the interface connected directly with the device. Instead, it is in another network segment, causing an IP address conflict.

If the client IP address is not in the connected network segment, the dynamic ARP table entries and directly connected routes are generated following ARP requests initiated by clients. In the following two cases (but not limited to the following two cases), clients cannot access the network and your client should re-learn the gateway IP address after clearing ARP table entries.

The device proxy responses the ARP request. After learning the device MAC address, dynamic ARP table entries and directly connected routes are cleared, the response packet cannot reach the client.

The device proxy responses the ARP request. The client disables any IP ARPand then enables it on the interface after the learning the devices MAC address.

Disabling any IP ARP will clear dynamic ARP table entries and directly connected routes, causing the response packet unable to reach the client.

If there are corresponding static ARP tables entries or ARP table entries of the VRRP IP address, dynamic ARP table entries generated by any IP ARP may be overwritten or not be added, causing any IP ARP failure.

Configuration Examples

The following example enables any IP ARP function.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# arp any-ip
```

The following example disables any IP ARP function.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# no arp any-ip
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.3 arp cache interface-limit

Use this command to set the maximum number of ARP learned on the interface.

Use the **no** form of this command to restore the default setting.

arp cache interface-limit *limit*

no arp cache interface-limit

Parameter Description

Parameter	Description
limit	Sets the maximum number of ARP learned on the interface, including static and dynamic ARPs, in the range from 0 to the number supported on the interface. 0 indicates that the number is not limited.

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide This function can prevent ARP attacks from generating ARP entries to consume memory. *limit* must be no smaller than the number of ARPs learned on the interface. Otherwise, the configuration does not take effect.

Configuration Examples The following example sets the maximum number of ARP learned on the interface to 300.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# arp cache interface-limit 300
```

The following example restores the default setting.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# no arp any-ip
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.4 arp gratuitous-send interval

Use this command to set the interval of sending the free ARP request message on the interface. Use the**no** form of this command to restore the default setting.

arp gratuitous-send interval *seconds*

no arp gratuitous-send

Parameter Description

Parameter	Description
seconds	The time interval to send the free ARP request message in the range from 1 to 3600 in the unit of seconds.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide

If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.

Configuration Examples

The following example sets to send one free ARP request to SVI 1 per second.

```
FS(config)# interface vlan 1
FS(config-if)# arp gratuitous-send interval 1
```

The following example stops sending the free ARP request to SVI 1.

```
FS(config)# interface vlan 1
FS(config-if)# no arp gratuitous-send
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.5 arp oob

Use this command to configure the static ARP on the management interface. Use the **no** form of this command to restore the default setting.

arp oob *ip-address mac-address type*

no arp oob *ip-address*

Parameter Description

Parameter	Description
ip-address	The IP address corresponding to the MAC address, written as four groups of dotted decimal values.
mac-address	The data link layer address, composed of 48 bits.
type	The ARP encapsulation type. The key word for the Ethernet interface is **arpa**.

Defaults

No static ARP is configured by default.

Command Mode

Global configuration mode

Usage Guide

FSOS uses the ARP cache table to search for the 48-bit MAC address according to the 32-bit IP address.

Most hosts support dynamic ARP analysis, so static ARP mapping does not need to be configured. The clear arp-cache oob command is used to clear the ARP mapping learned by the management port dynamically.

If no management interface is specified, the static ARP is configured on the first management interface by default. If you specify the first management interface, the *mgmt-name* parameter is not displayed by running the **show run** command.

Configuration Examples

The following example configures a static ARP mapping record for the Ethernet host

```
FS(config)# arp oob 1.1.1.1 4e54.3800.0002 arpa
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME.

2.6 arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. Use the **no** form of this command to restore the default setting.

arp retry interval *seconds*

no arp retry interval

Parameter Description

Parameter	Description
seconds	Time for retransmitting the ARP request message in the range from 1 to 3600 in the unit of seconds.

Defaults

The default is 1.

Command Mode

Global configuration mode.

Usage Guide

The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.

Configuration Examples

The following example sets the retry interval of the ARP request as 30 seconds.

```
FS(config)# arp retry interval 30
```

Related Commands

Command	Description
arp retry times	Number of times for retransmitting an ARP request message.

Platform Description

N/A

2.7 arp retry times

Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. Use the **no** form of this command to restore the default setting.

arp retry times *number*

no arp retry times

Parameter Description

Parameter	Description
number	The times of sending the same ARP request in the range from 1 to100.When

	it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent.

Defaults The default is 5.

Command Mode Global configuration mode.

Usage Guide The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.

Configuration Examples The following example sets the local ARP request not to be retried.

```
FS(config)# arp retry times 1
```

The following example sets the local ARP request to be retried for one time.

```
FS(config)# arp retry times 2
```

Related Commands

Command	Description
arp retry interval	Interval for retransmitting an ARP request message

Platform Description N/A

2.8 arp scan

Use this command to enable ARP scanning. Use the **no** form of this command to restore the default setting.

arp scan [*start-ip-address end-ip-address*]

no arp scan [*start-ip-address end-ip-address*]

Parameter Description

Parameter	Description
start-ip-address	Specifies the start IP address of the ARP scan range. The start IP address cannot be greater than the end IP address.
end-ip-address	Specifies the end IP address of the ARP scan range. The end IP address cannot be smaller than the start IP address.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This function is used together with the ARP turning function (from dynamic to static).

The IP address with neighboring ARP entries existing is not scanned.

If you know the allocated IP range with LAN, you can specify the ARP scan range. The number of the specified IP addresses cannot be greater than 1024.

The start/end IP address of the ARP scan range must be in the same subnet as the interface IP address.

If you do not specify the IP address range, only the primary IP subnet on the interface is scanned. The subnet mask cannot be smaller than 22 bits.

ARP scanning takes effect once configured. It cannot be saved for the next time use.

ARP scanning takes effect on only an UP L3 interface (The link is UP and the port is configured with an IP address).

Configuration Examples

The following example enables ARP scanning with the IP address range unspecified.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# arp scan
```

The following example enables ARP scanning with the IP address range specified.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# arp scan 1.1.1.1 1.1.1.10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.9 arp trusted

Use this command to set the maximum number of trusted ARP entries. Use the **no** form of this command to restore the default setting.

arp trusted *number*

no arp trusted

Parameter Description

Parameter	Description
number	Maximum number of trusted ARP entries.

Defaults

N/A

Command Mode

Global configuration mode.

Usage Guide

To make this command valid, enable the trusted ARP function firstly. The trusted ARP entries and other entries share the memory. Too much trusted ARP entries may lead to insufficient ARP entry space. In general, you should set the maximum number of trusted ARP entries according to your real requirements.

Configuration Examples

The following example sets 1000 trusted ARPs.

```
FS(config)# arp trusted 1000
```

Related Commands

Command	Description
service trustedarp	Enables the trusted ARP function.

Platform Description N/A

2.10 arp trusted aging

Use this command to set trusted ARP aging. Use the **no** form of this command to restore the default setting.

arp trusted aging

no arp trusted aging

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide Use this command to set trusted ARP aging. Aging time is the same as dynamic ARP aging time. Use the **arp timeout** command to set aging time in interface mode.

Configuration Examples N/A

Related Commands

Command	Description
service trustedarp	Enables trusted ARP function.

Platform Description N/A

2.11 arp trust-monitor enable

Use this command to enable egress gateway trusted ARP. Use the **no** form of this command to restore the default setting.

arp trust-monitor enable

no arp trust-monitor enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The egress gateway trusted ARP is different from GSN trusted ARP. With this function enabled, the device sends a unicast request for confirmation when learning an ARP table entry. The device learns the ARP table entry after receiving the response. When the device receives the ARP packet, only if the ARP table entry is aged or incomplete and the ARP packet is a response packet will the packet be handled. After egress gateway trusted ARP is enabled, the aging time of the ARP table entry turns to 60 seconds. After this function is disabled, the aging time restores to 3600 seconds.

Configuration Examples

The following example enables egress gateway trusted ARP.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# arp trust-monitor enable
```

The following example disables engress gateway trusted ARP.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# no arp trust-monitor enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.12 arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache. Use the **no** form of this command to restore the default setting.

arp timeout *seconds*

no arp timeout

Parameter Description

Parameter	Description
secondsv	The timeout is in the range from 0 to 2147483 in the unit of seconds.

Defaults

The default is 3600.

Command Mode

Interface configuration mode/Global configuration mode

Usage Guide

The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

Configuration Examples

The following example sets the timeout for the dynamic ARP mapping record that is learned dynamically from FastEthernet port 0/1 to 120 seconds.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# arp timeout 120
```

Related Commands

Command	Description
clear arp-cache	Clears the ARP cache list.

show interface	Displays the interface information.

Platform Description N/A

2.13 arp unresolve

Use this command to set the maximum number of the unresolved ARP entries. Use **no** form of this command to restore the default setting.

arp unresolve *number*

no arp unresolve

Parameter Description

Parameter	Description
number	The maximum number of the unresolved ARP entries in the range from 1 to the ARP table size supported by the device.

Defaults The default is the ARP table size supported by the device.

Command Mode Global configuration mode.

Usage Guide If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.

Configuration Examples The following example sets the maximum number of the unresolved items to 500.

```
FS(config)# arp unresolve 500
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.14 arp-learning

Use this command to enable ARP learning. Use the **no** form of this command to disable this function.

arp-learning enable

no arp-learning enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default

Command Mode Interface configuration mode

Usage Guide After the device learns the dynamic ARP and turns it to the static ARP through Web, it is recommended to enable ARP learning. Otherwise, it is not recommended to enable this function. If this function is disabled with dynamic ARP existing, you can turn dynamic ARP to static ARP through Web. You can also clear the dynamic ARP using the clear arp command to deny the specified user's access to Internet. Otherwise, the dynamic ARP will be aged and then cleared. After this function is disabled, the AnyIP function and trust ARP detection are disabled.

Configuration Examples The following example enables ARP learning.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# arp-learning enable
```

The following example disbales ARP learning.

```
FS(config)# interface gi 0/0
FS(config-if-GigabitEthernet 0/0)# no arp-learning enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.15 clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table.

clear arp-cache [**trusted**] [*ip* [*mask*]] | **interface** *interface-name*]

Parameter Description

Parameter	Description
trusted	Deletes trusted ARP entries. Dynamic ARP entries are deleted by default.
ip	Deletes ARP entries of the specified IP address. If *trusted* value is specified, trusted ARP entries are deleted; otherwise, all dynamic ARP entries are deleted which is the default.
mask	Deletes ARP entries in a subnet mask. If *trusted* value is specified, trusted ARP entries in the subnet mask are deleted; otherwise, all dynamic ARP entries are deleted. The dynamic ARP entry specified by the IP address is deleted by default.
interface *interface-name*	Deletes dynamic ARP entries on the specified interface. Dynamic ARP entries are deleted on all interfaces by default.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command can be used to refresh an ARP cache table.

On a NFPP-based (Network Foundation Protection Policy) device, it receives one ARP packet for every mac/ip address per second by default. If the interval of two **clear arp** times is within 1s, the second response packet will be filtered and the ARP packet will not be resolved for a short time.

Configuration Examples

The following example deletes all dynamic ARP mapping records.

```
FS# clear arp-cache
```

The following deletes the dynamic ARP entry 1.1.1.1.

```
FS# clear arp-cache 1.1.1.1
```

The following example deletes the dynamic ARP entry on interface SVI1.

```
FS# clear arp-cache interface Vlan 1
```

Related Commands

Command	Description
arp	Adds a static mapping record to the ARP cache table.

Platform Description

N/A

2.16 clear arp-cache oob

Use this command to clear dynamic ARP mapping records.

clear arp-cache oob [*ip* [*mask*]]

Parameter Description

Parameter	Description
ip	Clears the ARP table entriy of the specified IP address. All dynamic ARP table entries are cleared by default.
mask	Clears the ARP table entry within the specified subnet. The dynamic ARP table entry of the specified IP address (the previous parameter) is cleared by default.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

On a device supporting Network Foundation Protection Policy (NFPP), every MAC / IP address receives an ARP packet per second by default. If the **clear arp oob** command is run twice within one second, the second response packet may be filtered, causing ARP uanalysis for a short time.

Configuration Examples

The following example clears the cache table of dynamic ARP mapping records.

```
FS# clear arp-cache oob
```

The following example clears dynamic ARP table entry 1.1.1.1.

```
FS# clear arp-cache oob 1.1.1.1
```

The following example clears the dynamic ARP table entry within the specified subnet.

```
FS# clear arp-cache oob 1.0.0.0 255.0.0.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME.

2.17 ip proxy-arp

Use this command to enable ARP proxy function on the interface. Use the **no** form of this command to restore the default setting.

ip proxy-arp

no ip proxy-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Interface configuration mode.

Usage Guide

Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

Configuration Examples

The following example enables ARP on FastEthernet port 0/1.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# ip proxy-arp
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.18 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

show arp [*interface-type interface-number* | **trusted** [*ip* [*mask*]] | [**vrf** *vrf-name*] [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]]

Parameter Description

Parameter	Description
interface-type interface-number	Displays the ARP entry of a specified Layer-2 or Layer-3 port.
trusted	Displays the trusted ARP entries. Currently, only the global VRF supports the trusted ARP.
ip	Displays the ARP entry of the specified IP address. If **trusted** is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
mask	Displays the ARP entries of the network segment included within the mask. If **trusted** is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
static	Displays all the static ARP entries.
complete	Displays all the resolved dynamic ARP entries.
incomplete	Displays all the unresolved dynamic ARP entries.
mac-address	Displays the ARP entry with the specified mac address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the output result of the **show arp** command:

```
FS# show arp
Total Numbers of Arp: 7
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 0 0013.20a5.7a5f arpa VLAN 1
Internet 192.168.195.67 0 001a.a0b5.378d arpa VLAN 1
Internet 192.168.195.65 0 0018.8b7b.713e arpa VLAN 1
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.63 0 001a.a0b5.3990 arpa VLAN 1
Internet 192.168.195.62 0 001a.a0b5.0b25 arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
Protocol	Protocol of the network address, always to be Internet
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".

Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, ARPA for all Ethernet addresses
Interface	Interface associated with the IP addresses

The following example displays the output result of show arp 192.168.195.68

```
FS# show arp 192.168.195.68
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 1 0013.20a5.7a5f arpa VLAN 1
```

The following example displays the output result of **show arp** 192.168.195.0 255.255.255.0

```
FS# show arp 192.168.195.0 255.255.255.0
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.2 1 00d0.f8ff.f00e arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
Internet 192.168.195.1 0 00d0.f8a6.5af7 arpa VLAN 1
Internet 192.168.195.51 1 0018.8b82.8691 arpa VLAN 1
```

The following example displays the output result of **show arp** 001a.a0b5.378d

```
FS# show arp 001a.a0b5.378d
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.67 4 001a.a0b5.378d arpa VLAN 1
```

The following example displays the output result of **show arp static**

```
FS# show arp static
Protocol   Address   Age(min)   Hardware   Type    Interface           Origin
Internet   192.168.23.55      <static>   0000.0000.0010   arpa    VLAN 100    Configure
Internet   192.168.23.56      <static>   0000.0000.0020   arpa    VLAN 100    Authentication
Internet   192.168.23.57      <static>   0000.0000.0020   arpa    VLAN 100    DHCP-Snooping
2    static arp entries exist.
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.19 show arp counter

Use this command to display the number of ARP entries in the ARP cache table.

show arp counter

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the output result of the **show arp counter** command:

```
FS#sho arp counter
ARP Limit:                    75000
Count of static entries:    0
Count of dynamic entries: 1 (complete: 1    incomplete: 0)
Total:                        1
```

The meaning of each field in the ARP cache table is described in the following Table.

Parameter	Description
overlay	Indicates the number of VxLAN-related ARP entries.
underlayer	Indicates the number of VxLAN-irrelated ARP entries.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.20 show arp detail

Use this command to display the details of the Address Resolution Protocol (ARP) cache table.

show arp detail [*interface-type interface-number* | trusted [*ip* [*mask*]] | [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]

Parameter Description

Parameter	Description
interface-type interface-number	Displays the ARP of the layer 2 port or the layer 3 interface.
trusted	Displays the trusted ARP entries. Currently, only the global VRF supports the trusted ARP.
ip	Displays the ARP entry of the specified IP address.
ip mask	Displays the ARP entries of the network segment included within the mask.
mac-address	Displays the ARP entry of the specified MAC address.
static	Displays all the static ARP entries.
completev	Displays all the resolved dynamic ARP entries.
incomplete	Displays all the unresolved dynamic ARP entries.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the ARP details, such as the ARP type (Dynamic, Static, Local, Trust), the information on the layer2 port.

If you enter a *min_value g*reater than *max_value*, no error message is prompted. Instead, ARP entries corresponding to the subvlan are displayed.

Configuration Examples The following example displays arp details including InnerVLAN on products supporting QinQ termination:

```
FS# show arp detail
IP Address        MAC Address        Type        Age(min)    Interface   Port      SubVlan    InnerVlan
20.1.1.2          0020.0101.0002     Static      --          Te2/5       --        --
20.1.1.1          00d0.f822.33bb     Local       --          Te2/5       --        --
1.1.1.2           00d0.1111.1112     Dynamic     1           Vl2         Te2/1     4          300
1.1.1.1           00d0.f822.33bb     Local       --          Vl2         --        --
```

The following example displays description information on a device supporting configuration of description.

```
FS#sho arp detail
IP Address     MAC Address      Type      Age(min) Interface   Port   description
1.1.1.1        00d0.f822.33eb   Static    --       Gi0/0       --     To-lib
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
IP Address	IP address corresponding to the hardware address
MAC Address	hardware address corresponding to the IP address
Type	ARP type, includes the Static, Dynamic, Trust,Local
Age (min)	Age of the ARP learning, in minutes
Interface	Layer 3 interface associated with the IP addresses
Port	Layer2 port associated with the ARP
SubVLAN	SubVLAN corresponding to the ARP entries
Location	Local: ARP entries are generated or learned on the local device. Remore: ARP entries are synced from a remote gateway.
Description	Description of a static ARP.

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

2.21 show arp oob

Use this command to display the ARP cache table.

show arp oob [*ip* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]

Parameter Description

Parameter	Description
ip	Displays ARP table entries of the specified IP address.
mask	Displays ARP table entries within the IP subnet.
static	Displays all static ARP table entries.
complete	Displays all analyzed ARP table entries.
incomplete	Displays all unanalyzed ARP table entries.
mac-address	Displays ARP table entries of the specified MAC address.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the ARP cache table. The **complete** / **incomplete** key word represents analyzed / unanalyzed ARP table entries.

Configuration Examples The following example displays the outcome of the running the show arp oob command.

```
FS# show arp oob
Total Numbers of Arp: 7
Protocol   Address          Age(min)   Hardware         Type     Interface
Internet   192.168.195.68   0          0013.20a5.7a5f   arpa     mgmt 0
Internet   192.168.195.67   0          001a.a0b5.378d   arpa     mgmt 0
Internet   192.168.195.65   0          0018.8b7b.713e   arpa     mgmt 0
Internet   192.168.195.64   0          0018.8b7b.9106   arpa     mgmt 0
Internet   192.168.195.63   0          001a.a0b5.3990   arpa     mgmt 0
Internet   192.168.195.62   0          001a.a0b5.0b25   arpa     mgmt 0
Internet   192.168.195.5    --         00d0.f822.33b1   arpa     mgmt 0
```

The following example displays the outcome of running the **show arp oob** 192.168.195.68 command.

```
FS# show arp oob 192.168.195.68
Protocol   Address          Age(min)   Hardware         Type     Interface
Internet   192.168.195.68   1          0013.20a5.7a5f   arpa     mgmt 0
```

The following example displays the outcome of running the show arp oob 192.168.195.0 255.255.255.0.

```
FS# show arp 192.168.195.0 255.255.255.0
Protocol   Address          Age(min)   Hardware         Type     Interface
Internet   192.168.195.64   0          0018.8b7b.9106   arpa     mgmt 0
Internet   192.168.195.2    1          00d0.f8ff.f00e   arpa     mgmt 0
Internet   192.168.195.5    --         00d0.f822.33b1   arpa     mgmt 0
Internet    192.168.195.1       0              00d0.f8a6.5af7    arpa      mgmt 0
Internet    192.168.195.51      1              0018.8b82.8691    arpa      mgmt 0
```

The following example displays the outcome of running the show arp oob 001a.a0b5.378d command.

```
FS# show arp 001a.a0b5.378d
Protocol    Address              Age(min)    Hardware            Type      Interface
Internet    192.168.195.67      4               001a.a0b5.378d    arpa      mgmt 0
```

Field	Description
Protocol	Only "Internet" is available at present, which indicates the IP protocol.
Address	The IPv4 address.
Age(min)	The age of the table entry. For the local IP address, the field is displayed as '-'. For the static table entry, the field is displayed as <static>. For the dynamic table entry, the field indicates the time for which the table entry has been learned, in the unit of minutes.
Hardware	48-bit MAC address, written as a dotted triple of four-digit hexadecimal numbers.
Type	Only "arpa" is available at present.
Interface	The L3 interface corresponding to the ARP table entry. The field is NULL for static ARP table entries for the IP address of the static ARP is not within any network segment directly connected with the device.

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME.

2.22 show arp packet statistics

Use this command to display the statistics of ARP packets.

show arp packet statistics [*interface-name*]

Parameter Description

Parameter	Description
interface-name	Displays the statistics of ARP packets on the specified interface.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

The following example displays the output information of the command.

```
FS# show arp packet statistics
Interface Received Received Received Sent Sent
Name Requests Replies Others Requests Replies
--------- -------- -------- -------- -------- -------
VLAN 1 10 20 1 50 10
VLAN 2 5 8 0 10 10
VLAN 3 20 5 0 15 12
VLAN 4 5 8 0 10 10
VLAN 5 20 5 0 15 12
VLAN 6 20 5 0 15 12
VLAN 7 20 5 0 15 12
VLAN 8 5 8 0 10 10
VLAN 9 20 5 0 15 12
VLAN 10 20 5 0 15 12
VLAN 11 20 5 0 15 12
VLAN 12 20 5 0 15 12
```

Description of fields:

Field	description
Received Requests	Number of received ARP requests
Received Replies	Number of received ARP response messages
Received Others	Number of other received ARP packets
Sent Requests	Number of sent ARP requests
Sent Replies	Number of sent ARP requests

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A

2.23 show arp timeout

Use this command to display the aging time of a dynamic ARP entry on the interface.

show arp timeout

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

N/A.

Command Mode

Privileged EXEC mode

Usage Guide

N/A.

Configuration Examples

The following example displays the output of the **show arp timeout** command:

```
FS# show arp timeout
Interface arp timeout(sec)
---------------------- ----------------
VLAN 1     3600
```

The meaning of each field in the ARP cache table is described in Table 1.

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A

2.24 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

show ip arp

Parameter Description

Parameter	Description
N/A.	N/A.

Defaults

N/A.

Command Mode

Privileged EXEC mode.

Usage Guide

N/A.

Configuration Examples

The following example displays the output of **show ip arp**:

```
FS# show ip arp
Protocol Address Age(min)Hardware Type Interface
Internet 192.168.7.233 23 0007.e9d9.0488 ARPA FastEthernet 0/0
Internet 192.168.7.112 10 0050.eb08.6617 ARPA FastEthernet 0/0
Internet 192.168.7.79 12 00d0.f808.3d5c ARPA FastEthernet 0/0
Internet 192.168.7.1 50 00d0.f84e.1c7f ARPA FastEthernet 0/0
Internet 192.168.7.215 36 00d0.f80d.1090 ARPA FastEthernet 0/0
Internet 192.168.7.127 0 0060.97bd.ebee ARPA FastEthernet 0/0
Internet 192.168.7.195 57 0060.97bd.ef2d ARPA FastEthernet 0/0
Internet 192.168.7.183 -- 00d0.f8fb.108b ARPA FastEthernet 0/0
```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with “-”.
Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

Related Commands

Command	Description
N/A.	N/A.

Platform Description

N/A

3 IP Event Dampening Commands

3.1 dampening

Use this command to enable the IP event dampening function on the interface. Use the **no** or **default** form of this command to disable this function.

dampening [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]]

no dampening

default dampening

Parameter Description

Parameter	Description
half-life-period	Configures the half-life period of suppression penalty. The range is from 1 to 30. The unit is seconds. The default value is 5 seconds.
reuse-threshold	Configures the penalty threshold to unsuppress the interface. The range is from 1 to 20,000. The default value is 1,000.
suppress-threshold	Configures the penalty threshold to suppress the interface. The range is from 1 to 20,000. The default value is 2,000.
max-suppress	Configures the maximum suppress time. The range is from 1 to 255. The default value is 4 times of the *half-life-period.*
restart	Activates the restart penalty.
restart-*penalty*	Configures the initial penalty value on the interface. The range is from 1 to 20,000. The default value is 2,000.

Defaults IP event dampening is disabled by default.

Command mode Interface configuration mode.

Usage Guide This function will influence the modules of the directly-connected/host route, static route, dynamic route and VRRP. If one interface meets the configuration condition of this command, which is in the suppression status, the above influenced modules consider the status of this interface as DOWN, so as to delete the corresponding route and not transcieve the data packets on this interface.

Re-configuring the dampening command on the interface that has been configured this command makes all dampening information on this interface cleared. However, the interface flapping times will be remained unless use the clear counters command to clear the statistical information of the interface.

Too small max-suppress configured may cause the maximum penalty value obtained from the calculation smaller than the suppression threshold to make this interface will not be suppressed forever. Therefore, it belongs to the erroneous configuration. In this case, the following message will prompt for the configuration error:

```
% Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time
```

Besides, when configuring this command, it will prompt the following message as well if the system memory is not enough to save this configuration:

```
% No memory, configure dampening fail!
```

For the interface layer switching of the switches (Layer-3 interface to the Layer-2 interface), for example, if one routed port is switched to the switch port, the dampening command configured on this interface will be removed.

Note: For routers, this function can be configured on the master interface only. This function takes effect for all sub-interfaces of the master interface with this command configured, but this command cannot be configured on the sub-interface directly. This command cannot be configured on the virtual template.

Configuration Examples

The following example configures the IP event dampening function.

```
FS(config)#interface gigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# no switchport
FS(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
show dampening interface	Displays the statistics of the dampening interface.
show interface dampening	Displays details of the dampening interface.

Platform Description

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.

3.2 show dampening interface

Use this command to show the statistics of the dampening interface.

show dampening interface

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode/ global configuration mode/ interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the statistics of the dampening interface.

```
FS# show dampening interface
3 interfaces are configured with dampening.
No interface is being suppressed.
```

Related Commands

Command	Description

dampening	Enables the IP event dampening function on the interface.
clear counters	Clears the interface counters.
show interface dampening	Displays details of IP event dampening configuration.

Platform Description

N/A

3.3 show interface dampening

Use this command to display the details of IP event dampening configuration.

show interface [*interface-Id*] **dampening**

Parameter Description

Parameter	Description
interface-id	Interface name

Defaults

N/A

Command mode

Privileged EXEC mode/ global configuration mode/ interface configuration mode

Usage Guide

If the interface-id is specified, only the dampening information of this specified interface is displayed.

Configuration Examples

The following example shows the details of IP event dampening configuration.

```
FS# show interface dampening Ethernet1/0
Flaps   Penalty   Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart
 0        0        FALSE    0        5      1000   2000    20      16000     0
```

Domain	Description
Flaps	Interface flapping times.
Penalty	The current penalty value on the interface.
Supp	Suppressed or not.
ReuseTm	Time to unsuppress the interface, in seconds.
HalfL	Half-life period, in seconds.
ReuseV	Unsuppressed threshold.
SuppV	Start suppression threshold.
MaxSTm	Maximum suppression time.
MaxP	Maximum penalty value.
Restart	The initial penalty value on the interface.

Related Commands

Command	Description

dampening	Enables the IP event dampening function.
clear counters	Clears the interface counters.
show dampening interface	Displays statistics of the dampening interface.

Platform Description N/A

4 TCP Commands

4.1 ip tcp adjust-mss

Use this command to change the Maximum Segment Size (MSS) option value of SYN packets sent and received on an interface. Use the **no** form of this command to restore the default setting.

ip tcp adjust-mss *max-segment-size*

no ip tcp adjust-mss

Parameter Description

Parameter	Description
max-segment-size	Maximum segment size in the range from 500 to 1460 bytes

Defaults

The MSS option value of SYN packets is not changed by default.

Command Mode

Interface configuration mode

Usage Guide

MSS refers to the maximum size of the payload of a TCP packet.

The TCP Path MTU (PMTU) is implemented as per RFC1191. This feature can improve the network bandwidth utilization ratio. When the user uses TCP to transmit mass data, this feature can substantially enhance the transmission performance.

When the client initiates a TCP connection, it negotiates the maximum payload of TCP packets through the MSS option field of the TCP SYN packet. The MSS value of the client's SYN packet implies the maximum payload of TCP packets sent by the server, and vice versa.

Configuring this command on the interface will change the MSS option of SYN packets received or sent by the interface to the MSS value configured on the interface. If the MSS is configured on both the inbound interface and the outbound interface of the SYN packet, the smaller of the two applies. It is recommended that you configure the same value on the inbound interface and outbound interface.

This command actually changes the SYN packet exchanged during TCP connection establishment. For some versions, this command may also change the SYN+ACK packet.

This command takes effect on the subsequent TCP connections to be established instead of established TCP connections.

Configuration Examples

The following example changes the MSS option value of the TCPv4 SYN packet to 1000 bytes on port GigabitEthernet 0/0.

```
FS(config-if-GigabitEthernet 0/0)# ip tcp adjust-mss 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.2 ip tcp mss

Use this command to set the upper limit of the MSS value. Use the **no** form of this command to restore the default setting.

ip tcp mss *max-segment-size*

no ip tcp mss

Parameter Description

Parameter	Description
max-segment-size	Upper limit of the MSS value in the range from 68 to 10000 bytes

Defaults The default MSS = Outgoing IPv4/v6 MTU- IPv4/v6 header-TCP header.

Command Mode Global configuration mode

Usage Guide This command is used to limit the maximum value of MSS for the TCP connection to be created. The negotiated MSS cannot exceed the configured value. You can use this command to reduce the maximum value of MSS. However, this configuration is not needed in general. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples The following example sets the upper limit of the MSS value to 1300 bytes.

```
FS(config)# ip tcp mss 1300
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.3 ip tcp path-mtu-discovery

Use this command to enable Path Maximum Transmission Unit (PMTU) discovery function for TCP in global configuration mode. Use the **no** form of this command to restore the default setting.

ip tcp path-mtu-discovery [**age-timer** *minutes* **| age-timer infinite**]

no ip tcp path-mtu-discovery

Parameter Description

Parameter	Description
age-timer *minutes*	The time interval for further discovery after discovering PMTU. Its value ranges from 10 to 30 minutes. The default value is 10.
age-timer infinite	No further discovery after discovering PMTU

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Based on RFC1191, the TCP path MTU function improves the network bandwidth utilization and data transmission when the user uses TCP to transmit the data in batch.

Enabling or disabling this function takes no effect for existent TCP connections and is only effective for TCP connections to be created. This command applies to only IPv4 TCP. This function is enabled for IPv6 TCP constantly and cannot be disabled.

According to RFC1191, after discovering the PMTU, the TCP uses a greater MSS to detect the new PMTU at a certain interval, which is specified by the parameter **age-timer**. If the PMTU discovered is smaller than the MSS negotiated between two ends of the TCP connection, the device will be trying to discover the greater PMTU at the specified interval untill the PMTU value reaches the MSS or the user stops this timer. Use the parameter **age-timer infinite** to stop this timer.

Configuration Examples The following example enables PMTU discovery.

```
FS(config)# ip tcp path-mtu-discovery
```

Related Commands

Command	Description
show tcp pmtu	Shows the PMTU value for the TCP connection.

Platform Description N/A

4.4 ip tcp send-reset

Use this command to enable the device to send the reset packet when receiving the TCP port unreachable packet. Use the **no** form of this command to disable this function,

ip tcp send-reset

no ip tcp send-reset

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Global configuration mode

Usage Guide In general, when dispatching the TCP packet, the TCP module replies a reset packet automatically to disconnect the TCP connection with the peer end if the TCP connection that this packet belongs to is not found, However, flooding TCP port unreachable packets pose an attack threat to the device, This command can be used to disable the device from sending the reset packet when receiving the TCP port unreachable packet. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples

The following example disables the device from sending the reset packet when receiving the TCP port unreachable packet.

```
FS(config)# no ip tcp send-reset
```

Related Commands

CommandFSOS	**Description**
N/A	N/A

Platform Description

The **ip tcp not-send-rst** command in 10.x is compatible in FSOS 11.0. When you run this command, it is converted to the **no ip tcp send-reset** command automatically.

4.5 ip tcp keepalive

Use this command to enable the TCP keepalive function. Use the **no** form of this command to restore the default setting,

ip tcp keepalive [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]

no ip tcp keepalive

Parameter Description

Parameter	**Description**
interval *num1*	The interval of sending the keepalive packet, in the range from1 to 120 in the unit of seconds, The default is 75.
times *num2*	Keepalive packet sending times, in the range from 1 to 10. The default is 6.
idle-period *num3*	Idle time, the time period during which the peer end does not send any packet to the local end, in the range from 60 to 1800 in the unit of seconds. The default is 900.

Defaults

The function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

The keepalive function enables TCP to detect whether the peer end is operating properly.

Suppose the keepalive function is enabled together with default **interval**, **times** and **idle-period** settings. TCP begins to send the keepalive packet at an interval of 75 seconds if it does not receive any packet from the peer end in 900 seconds. The TCP connection is considered invalid and then disconnected automatically if the device sends the keepalive packet for six consecutive times without receiving any TCP packet from the peer end. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples

The following example enables the TCP keepalive function on the device and sets the **idle-period** and **interval** to180 and 60 respectively. If the device sends the keepalive packet for four consecutive times without receiving any TCP packet from the peer end, the TCP connection is considered invalid.

```
FS(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

Related Commands

Command	Description
N/A	N/A

Platform Description

When you run the FSOS 10.x command **service tcp-keepalives-in** or **service tcp-keepalives-out**, it is converted to this command automatically in FSOS 11.0.

4.6 ip tcp synwait-time

Use this command to set the timeout value for SYN packets (the maximum time from SYN transmission to successful three-way handshake). Use the **no** form of this command to restore the default setting.

ip tcp synwait-time *seconds*

no ip tcp synwait-time *seconds*

Parameter Description

Parameter	Description
seconds	Timeout value for SYN packets in the range from 5 to 300 in the unit of seconds.

Defaults

The default is 20.

Command Mode

Global configuration mode

Usage Guide

If there is an SYN attack in the network, reducing the SYN timeout value can prevent resource consumption, but it takes no effect for successive SYN attacks. When the device actively requests a connection with an external device, reducing the SYN timeout value can shorten the time for the user to wait, such as telnet login. For poor network conditions, the timeout value can be increased properly. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples

The following example set the timeout value for SYN packets to 10 seconds.

```
FS(config)# ip tcp syntime-out 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.7 ip tcp window-size

Use this command to change the size of receiving buffer and sending buffer for TCP connections. Use the **no** form of this command to restore the default setting.

ip tcp window-size *size*

no ip tcp window-size

Parameter Description

Parameter	**Description**
size	Size of receiving buffer and sending buffer for TCP connections in the range from 128 to 65535 << 14 bytes.

Defaults

The default is 65535.

Command Mode

Global configuration mode

Usage Guide

The TCP receiving buffer is used to buffer the data received from the peer end. These data will be subsequently read by application programs. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For connections involving a large bandwidth and mass data, increasing the size of receiving buffer will remarkably improve TCP transmission performance.

The sending buffer is used to buffer the data of application programs. Each byte in the sending buffer has a sequence number, and bytes with sequence numbers acknowledged will be removed from the sending buffer. Increasing the sending buffer will improve the interaction between TCP and application programs, thus enhancing the performance. However, increasing the receiving buffer and sending buffer will result in more memory consumption of TCP.

This command is used to change the size of receiving buffer and sending buffer for TCP connections.

This command changes both the receiving buffer and sending buffer, and only applies to subsequent connections. This command applies to both IPv4 and IPv6 TCP.

Configuration Examples

The following example sets the TCP window size to 16386 bytes.

```
FS(config)# ip tcp window-size 16386
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

4.8 service tcp-keepalives-in

Use this command to enable the keepalive function for the TCP server. Use the no form of this command to restore the default setting.

service tcp-keepalives-in [*interval*] [**garbage**]

no service tcp-keepalives-in

Parameter Description

Parameter	Description
interval	The interval of sending keepalive packets, in the range from 1 to 65535 in the unit of seconds. The default is 60.
garbage	The keepalive packet contains one-byte invalid data. The invalid data is not contained by default.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide The keepalive function enables the TCP server to detect whether the client is operating properly.

If the TCP server sends the keepalive packet for four consecutive times without receiving any TCP packet from the client, the TCP connection is considered invalid and then is disconnected automatically.

Configuration Examples The following example enables the keepalive function for the TCP server and sets the interval of sending the keepalive packet to 10 seconds. The keepalive packet contains one-byte invalid data.

```
FS(config)# service tcp-keepalives-in 10 garbage
```

Related Commands

Command	Description
N/A	N/A

Platform Description When you run this FSOS 10.x command, it is converted to the **ip tcp keepalive** command automatically in FSOS 11.0.

4.9 service tcp-keepalives-out

Use this command to enable the keepalive function for the TCP client. Use the **no** form of this command to restore the default setting,

service tcp-keepalives-out [*interval*] [**garbage**]

no service tcp-keepalives-out [*interval*] [**garbage**]

Parameter Description

Parameter	Description
interval	The interval of sending keepalive packets, in the range from 1 to 65535 in the unit of seconds. The default is 60.
garbage	The keepalive packet contains one-byte invalid data. The invalid data is not contained by default.

Defaults This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

The keepalive function enables the TCP client to detect whether the server is operating properly.

If the TCP client sends the keepalive packet for four consecutive times without receiving any TCP packet from the server, the TCP connection is considered invalid and then is disconnected automatically.

Configuration Examples

The following example enables the keepalive function for the TCP client and sets the interval of sending the keepalive packet to 10 seconds. The keepalive packet contains one-byte invalid data

```
FS(config)# service tcp-keepalives-out 10 garbage
```

Related Commands

Command	Description
N/A	N/A

Platform Description

When you run this FSOS 10.x command, it is converted to the **ip tcp keepalive** command automatically in FSOS 11.0.

4.10 show tcp connect

Use this command to display basic information about the current TCP connections.

show tcp connect [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]

Use this command to display the current IPv4 TCP connection statistics.

show tcp connect statistics

Parameter Description

Parameter	Description
local-ip *a.b.c.d*	Local IP address.
local-port *num*	Local port.
peer-ip *a.b.c.d*	Peer IP address.
peer-port *num*	Peer port.
statistics	Displays IPv4 TCP connection statistics.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the current IPv4 TCP connection information.

```
FS#show tcp connect
```

```
Number Local Address        Foreign Address              State           Process name
1          0.0.0.0:22              0.0.0.0:0                          LISTEN          fs-sshd
2          0.0.0.0:23              0.0.0.0:0                          LISTEN          fs-telnetd
3          1.1.1.1:23              1.1.1.2:64201                   ESTABLISHED fs-telnetd
```

Field	Description
Number	Sequence number.
Local Address	The Local address and port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23" , "23" is the port number.
Foreign Address	The remote address and port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23" , "23" is the port number.
State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.
Process name	Process name.

The following example displays the current IPv4 TCP connection statistics.

```
FS#show tcp connect statistics
State         Count
-----            -----
ESTABLISHED 1
SYN_SENT     0
SYN_RECV     0
FIN_WAIT1    0
FIN_WAIT2    0
TIME_WAIT    0
```

```
CLOSED        0
CLOSE_WAIT    0
LAST_ACK      0
LISTEN        1
CLOSING       0
Total: 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.11 show tcp parameter

Use this command to show TCP parameters.

show tcp parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example shows TCP parameters.

```
FS#show tcp parameter
Hash table information:
  Established hash bucket size: 16384
  Bind hash bucket size: 16384
Memory information:
  Global memory limit: low=92160, pressure=122880, high=184320 (unit: pages)
  Per-socket receive buffer size: min=4096, default=87380, max=3932160 (unit: bytes)
  Per-socket send buffer size: min=4096, default=16384, max=3932160 (unit: bytes)
  Current allocated memory: 0
  Current memory pressure flag: 0
SYN specific information:
  Max SYN_RECV sockets per LISTEN socket: 65535
```

```
    Max SYN retries: 5
    Max SYN ACK retries: 5
Timewait specific information:
    Max timewait sockets: 180000
    Current timewait sockets: 0
    Timewait recycle: 0
    Reuse timewait port: 0
Keepalive information:
    Keepalive on: 0
    Idle period: 900 seconds
    Interval: 75 seconds
    Max probes: 6
MTU probing:
    Enable mtu probing: 0
FIN specific information:
    FIN_WAIT_2 timeout: 60 seconds
Orphan socket information:
    Max orphans: 16384
    Max orphan retries: 0
Current orphans: 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.12 show tcp pmtu

Use this command to display information about TCP PMTU.

show tcp pmtu [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]

Parameter Description

Parameter	Description
local-ip *a.b.c.d*	Local IP address.
local-port *num*	Local port.
peer-ip *a.b.c.d*	Peer IP address.
peer-port *num*	Peer port.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays PMTU of IPv4 TCP connection.

```
FS# show tcp pmtu
Number    Local Address                Foreign Address              PMTU
1         192.168.195.212.23           192.168.195.112.13560    1440
```

Field	Description
Number	Sequence number.
Local Address	The local address and the port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23" , "23" is the port number.
Foreign Address	The remote address and the port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23" , "23" is the port number.
PMTU	PMTU value.

Related Commands

Command	Description
ip tcp path-mtu-discovery	Enables the TCP PMTU discovery function.

Platform Description N/A

4.13 show tcp port

Use this command to display information about the current TCP port.

show tcp port [*num*]

Parameter Description

Parameter	Description
num	Port number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the current IPv4 TCP port status.

```
FS#sh tcp port
tcp port status:
```

```
Tcpv4 listen on 2650 have connections:
TCB          Foreign Address                             Port       State
Tcpv4 listen on 2650 have total 0 connections.
Tcpv4 listen on 23 have connections:
TCB          Foreign Address                             Port       State
c340800      1.1.1.2                                     64571      ESTABLISHED
Tcpv4 listen on 23 have total 1 connections.
Tcpv6 listen on 23 have connections:
TCB          Foreign Address                             Port       State
c429980      3000::2                                     64572      ESTABLISHED
```

Tcpv6 listen on 23 have total 1 connections.

Field	Description
TCB	The control block's location in the current memory
Foreign Address	Remote address
Port	Remote port number
State	Status of the current TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.14 show tcp statistics

Use this command to show TCP statistics on received packets, three way handshake and time-wait.

show tcp parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example shows TCP parameters.

```
FS#show tcp statistics
TCP Packets
    Received: 1103
    Errors     : 0(checksum: 0)
Three way handshake
    Request queue overflow: 0
    Accept backlog full: 0
    Web authentication limit per user: 0
    Failed to alloc memory for request sock: 0
    Failed to create open request child: 0
    SYN ACK retransmits: 0
    Timeouted requests: 0
Time-wait
    Time-wait bucket table overflow: 0
```

Field Description

Field	Description
TCP Packets	Normal packets and error packets
Three way handshake	Three way handshake information, including session request count, server-client connection count, three way handshake failure count caused by Web authentication limit, TCP socket failure count caused by memory shortage, sub-session failure count, packet retransmission count and session failure count caused by retransmission timeout.
Time-wait	Session in TIMEWAIT state

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

5 IPv4/IPv6 REF Commands

5.1 clear ip ref packet statistics

Use this command to clear IPv4 FS Express Forwarding (REF) packet statistics.

clear ip ref packet statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears IPv4 REF packet statistics.

```
FS#clear ip ref packet statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.2 ip ref load-sharing original

Use this command to configure the algorithm that is used for load balancing during forwarding based on the source and destination IPv4 addresses. Use the **no** form of this command to restore the default setting.

ip ref load-sharing original

no ip ref load-sharing original

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default algorithm is based on the destination IPv4 address.

Command Mode Global configuration mode

Usage Guide The REF is responsible for data forwarding and supports two load balancing algorithms. One is based on destination IP addresses and the other is based on the source and destination IP addresses. When IP packets are forwarded on multiple paths, for example, when load balancing based on destination IP addresses is configured, the REF forwards packets based on a path matching the destination IP address of packets. By default, load balancing based on destination IP addresses is used.

Configuration Examples

The following example configures the load balancing algorithm based on source and destination IP addresses.

```
FS(config)# ip ref load-sharing original
```

The following example configures the load balancing algorithm based on destination IP addresses of packets.

```
FS(config)# no ip ref load-sharing original
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.3 show ip ref adjacency

Use this command to display the information about the specified adjacent node or all adjacent nodes.

show ip ref adjacency [**glean** | **local** | *ip-address* | **interface** *interface_type interface_number* | **discard** | **statistics**]

Parameter Description

Parameter	Description
glean	Aggregate adjacent node, which is used for a direct route
local	Local adjacent node, which is used by the local host
Ip-address	Next-hop IP address
interface_type	Interface type
interface_number	Interface number
discard	Displays discarded adjacent nodes.
statistics	Statistics

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command can be used to display the information about the adjacent node table in the current REF module. By specifying parameters, the information about the aggregate adjacent node, local adjacent node, adjacent node of the specified IP address, adjacent node associated with the specified interface, and all adjacent nodes can be displayed.

Configuration Examples

The following example displays the information about all adjacent nodes in the adjacent node table. FS#show ip ref adjacency

```
id state         type     rfct chg    ip                interface            linklayer(header data)
1   unresolved mcast   1      0     224.0.0.0
```

```
9    resolved     forward 1       0      192.168.50.78      GigabitEthernet 0/0    00 25 64 C5 9D 6A 00 D0 F8 98 76 54
08 00
7    resolved     forward 1       0      192.168.50.200    GigabitEthernet 0/0    00 04 5F 87 69 66 00 D0 F8 98 76 54 08
00
6    unresolved    glean    1       0      0.0.0.0                GigabitEthernet 0/0
4    unresolved    local    3       0      0.0.0.0                Local 1
```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

Related Commands

Command	Description
show ip ref route	Displays all route information in the current REF module.

Platform Description

N/A

5.4 show ip ref exact-route

This command is used to display the IPv4 REF exact route.

show ip ref exact-route [**oob**] *source_ipaddress dest_ipaddress*

Parameter Description

Parameter	Description
oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
source_ipaddress	Source IP address of the packet
dest_ipaddress	Destination IP address of the packet

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to specify the source and the destination IP address of the IP packets, and to display the path of forwarding the current packet with REF

Configuration Examples

The following example displays the IPv4 REF exact route from 192.168.217.74 to 192.168.13.1.

```
FS# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74    --> 192.168.13.1:
id state        type       rfct chg    ip                   interface                linklayer(header data)
9    resolved forward 1          0      192.168.17.1    GigabitEthernet 0/0 00 25 64 C5 9D 6A 00 D0 F8 98 76 54 08 00
```

Description of fields:

Field	Description
id	Adjacency ID
state	Adjacency state: Unresolved Resolved
type	Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacency
chg	Whether the adjacency is on the changing link.
ip	Adjacency IP address
interface	Interface
linklayer	Layer 2 head

Related Commands

Command	Description
show ip ref route	Displays all routing information in the current REF module.

Platform Description

This command is supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME.

5.5 show ip ref packet statistics

Use this command to display IPv4 REF packet statistics.

show ip ref packet statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays IPv4 REF packet statistics.

```
FS #show ip ref pkt-statistic
ref packet statistic:
     bad head            : 0
     lookup fib fail : 0
     local adj          : 0
     glean adj           : 0
     forward              : 0
     redirect            : 0
     punt adj             : 0
     outif not in ef : 0
     ttl expiration    : 0
     no ip routing      : 0
```

Field	Description
bad head	Number of the packets with false header
lookup fib fail	Number of the packets with failed REF routing
local adj	Number of the packets matching the local adjacency
glean adj	Number of the packets matching the gleaned adjacency
forward	Number of the packets matching the forwarded adjacency
redirect	Number of the redirected packets.
ttl expiration	Number of the packets exceeding the TTL.
no ip routing	Number of the packets not allowed to be forwarded and sent to local.

Related Commands

Command	Description

N/A	N/A

Platform Description

N/A

5.6 show ip ref resolve-list

Use this command to display the IPv4 REF resolution information.

show ip ref resolve-list

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays IPv4 REF resolution information.

```
FS#show ip ref resolve-list
IP                        res_state flags interface
1.1.1.1                 unres       1         GigabitEthernet 0/0
```

Field	Description
IP	IP address
res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.7 show ip ref route

Use this command to display all the routing information in the IPv4 REF table.

show ip ref route [**oob**] [**default** | *ip mask* | **statistics**]

Parameter

Parameter	Description

Description

oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
default	Specifies the default route.
ip	Specifies the destination IP address of the route
mask	Specifies the mask of the route.
statistics	Statistics

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the related routing information on the current REF table, and specify the default route and all the routing information matching IP/MASK.

Configuration Examples

The following example displays all the routing information in the IPv4 REF table.

```
FS#show ip ref route
Codes: * - default route
       # - zero route
 ip          mask       weight   path-id          next-hop              interface
 255.255.255.255 255.255.255.255 1    4      0.0.0.0          Local 0
 224.0.0.0               240.0.0.0                 1    1      224.0.0.0
 224.0.0.0            255.255.255.0        1    4         0.0.0.0          Local 0
 192.168.50.0    255.255.255.0           1    6      0.0.0.0 FastEthernet 0/0
 192.168.50.255    255.255.255.255 1    2             0.0.0.0
 192.168.50.200 255.255.255.255 1 7 192.168.50.200 FastEthernet 0/0
 192.168.50.122    255.255.255.255 1 4 0.0.0.0                 Local 0
 192.168.50.78    255.255.255.255 1 9 192.168.50.78    FastEthernet 0/0
```

Field	Description
ip	Destination IP address
mask	Mask
path-id	Adjacent identity
next-hop	Address of next hop
weight	Routing weight
interface	Egress

Related Commands

Command	Description
show ip ref exact-route	Displays the accurate REF forwarding path of an IP packet.

Platform Description	This command is supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME

6 Tunnel Commands

6.1 show interfaces tunnel

Use this command to display the tunnel configuration.

show interfaces tunnel [*number*]

Parameter Description

Parameter	Description
number	Specifies the tunnel number.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays tunnel 1 information.

```
FS#showinterfaces tunnel 1
// Here is the public information about the interface
Tunnel source 1.1.1.2, destination 1.1.1.1, routeable
   Tunnel TOS/Traffic Class not set, Tunnel TTL 254
   Tunnel config nested limit is 0, current nested number is 0
   Tunnel protocol/transport is ipv6ip
   Tunnel transport VPN is no set
```

Field Description

Field	Description
Destination	The tunnel destination address. The address 0.0.0.0 indicates that the destination address is not configured.
Tunnel source	The tunnel source address, which can be either an IPv4 or an IPv6 address. If the **tunnel source interface**command is configured, the tunnel source address is the interface address.
Tunnel TTL	The TTL or hop limit field of the transmission protocol.
Tunnel TOS	The TOS or traffic class field of the transmission protocol. Note that there is an exception. If the field is 0, and the transmission protocol is the same as the payload protocol, the field of the payload protocol is copied to the transmission protocol.
Tunnel nested-limit	The limit to the number of tunnel nested encapsulation times. This filed is displayed by all

	tunnels except the 6to4, 6rd and isatap tunnels.
Tunnel protocol/transport	Tunnel encapsulation mode
Key	With the key setting, this field is displayed by only the GRE tunnel.
Checksuming	With the checksum setting, this filed is displayed by only the GRE tunnel.
Tunnel VPN	The destination VRF.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.2 show tunnel statistics

Use this command to display the number of configurable tunnel interfaces and configured tunnel interfaces.

show tunnel statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

This command is used to display the number of configurable tunnel interfaces and configured tunnel interfaces. Note that the actual forwarding capacity is restricted by the number of chipentries. It is possible that the tunnel interface has been created while the chip entry list is full. In that case, the syslog is generated.

Configuration Examples

The following example displays the number of configurable tunnel interfaces and configured tunnel interfaces.

```
FS#show tunnel statistics
used: 2,    limit: 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.3 tunnel destination

Use this command to specify the destination IP address of a tunnel interface in interface configuration mode.

Use the **no** form of this command to restore the default setting.

tunnel destination*ip-address*

no tunnel destination

Parameter Description

Parameter	Description
ip-address	Sets the IP address of the specified tunnel destination.

Defaults Nodestination IP address is setby default.

Command Mode Interface configuration mode

Usage Guide This command must be used to specify the peer address during tunnel setup. Tunnels cannot be set up if this command is not executed.

Configuration Examples The following example sets the destination IP address of tunnel interface0 to 61.154.101.3.

```
FS(config)# interface tunnel0
FS(config-if)# tunnel destination61.154.101.3
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

6.4 tunnel mode

Use this command to set the encapsulation mode on a tunnel interface.

Use theno ordefaultform of this command to restore to the default setting.

tunnel mode { gre{ip|ipv6} | ipip| ipv6ip}

no tunnel mode

default tunnel mode

Parameter Description

Parameter	Description
gre ip	GRE for the route at the IP layer
gre ipv6	GRE for the route at the IPv6 layer
ipip	IP over IP encapsulation mode
ipv6ip	IPv6 over IP encapsulation mode

Defaults

For switches and wireless products, the default encapsulation mode is **ipv6ip**.

For gateways and routers, the default encapsulation mode is **gre ip**.

Command Mode

Interface configuration mode

Usage Guide

The tunnel encapsulation format is the tunnel carrier protocol. The default encapsulation format of tunnel interfaces is GRE. You can determine the encapsulation format of tunnel interfaces based on the actual usage. By default, IP tunnel GRE can be implemented without any definition of the encapsulation format.

Configuration Examples

The following example encapsulates GRE IP on tunnel interface 0.

```
FS(config)# interface tunnel 0
FS(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description

N/A

6.5 tunnel source

Use this command to configurethe source IP address for the tunnel.

Use the **no** form of this command to restore the default setting.

tunnel source { *ip-address* **|** *interface-type interface-number* **}**

no tunnel source

Parameter Description

Parameter	Description
ip-address	Source IP address of the tunnel used as the source IP address of the packets to be transmitted through the tunnel.
interface-type interface-number	Interface referenced by the tunnel, which will be used as the source IP address of the packets to be transmitted through the tunnel.

Defaults

No tunnel source address is configured by default.

Command Mode

Interface configuration mode.

Usage Guide

The source IP address of a tunnel can be a specified IP address or an IP address of an interface. When you configure an auto tunnel (for example, 6to4 and isatap), it is recommended to specify the source address.

A device shall not be configured multiple tunnels with the same encapsulation type, source address and destination address.

If there are multiple auto tunnels, their source addresses shall be different.

Configuration Examples

The following example configures an IPv6 manual tunnel.

```
FS(config)# interface tunnel 1
FS(config-if)# tunnel mode ipv6ip
FS(config-if)# tunnel source vlan 1
FS(config-if)# tunnel destination 192.168.5.1
```

Related Commands

Command	Description
tunnel mode	Configures the mode of a tunnel.
tunnel destination	Configures the destination address of a tunnel.
Tunnel ttl	Configures the TTL of the tunnel.

Platform Description

N/A

6.6 tunnel tos

Use this command to set the IPv4 ToS byte or IPv6 traffic class 8 bits fin tunnel intefface configruation mode. Use the **no** form of this command to restore the default setting.

tunnel tos[*number*]

no tunnel tos

Parameter Description

Parameter	Description
number	IPv4 ToS byte or IPv6 traffic class 8 bits, in the range from 0 to 255.

Defaults

By default, the inner-layer IPv4 ToS byte is copied to the outer-layer IPv4 header, if both the inner-layer carrier and the outer-layer encapsulation on a tunnel interface use the IPv4 protocol. By default, the inner-layer IPv6 traffic class 8 bits are copied to the outer-layer IPv6 header if both the inner-layer carrier and the outer-layer encapsulation on a tunnel interface use the Ipv6 protocol.

In other circumstances, the outer-layer IPv4 ToS and IPv6 traffic class are 0.

Command Mode

Interface configuration mode

Usage Guide

This command is used to set GRE tunnel packets to a higher priority.

Configuration Examples

The following example sets the ToS byte for a GRE tunnel outer-layer encapsulation protocol to 20 on interface tunnel 1.

```
FS(config)# interface tunnel 1
FS(config-if)# tunnel mode ipv6ip
FS(config-if)# tunnel tos 20
```

Related Commands

Command	Description
show interface tunnel	Displays tunnel interface information.

Platform Description N/A

6.7 tunnel ttl

Use this command to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages. Use the**no** form of this command to restore the default setting.

tunnel ttl*hop-count*

no tunnel ttl

Parameter Description

Parameter	Description
hop-count	TTL value

Defaults The default is 254.

Command Mode Interface configuration mode

Usage Guide This command is used to specify the TTL value of the IPv4 header in the encapsulated IPv6 messages.

Configuration Examples

```
FS(config)# interface tunnel1
FS(config-if)# tunnel mode ipv6ip
FS(config-if)# tunnel ttl 64
```

Related Commands

Command	Description
tunnel mode	Configures the mode of a tunnel.
tunnel source	Configures the source IP address of the tunnel.
tunnel destination	Configures the destination IP address of a tunnel.

Platform Description N/A

6.8 tunnel 6rd br

Use this command to configure the IPv4 address for 6rd br.

Use the **no** form of this command to remove the configuration.

tunnel 6rd br*ipv4-address*

no tunnel 6rd br

Parameter Description

Parameter	Description
ipv4-address	The IPv4 address.

Defaults N/A

Command Mode

Interface configuration mode

Usage Guide

This command is used to configure the IPv4 address for the 6rd relay router.

Configuration Examples

The following example configures the IPv4 address for tunnel 6rd br .

```
FS# configureterminal
FS(config)# interface tunnel 100
FS(config-if-Tunnel 100)# ipv6 enable
FS(config-if-Tunnel 100)# tunnel 6rd br 10.1.2.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is not supported on switches.

6.9 tunnel 6rd ipv4

Use this command toconfigure the common IPv4 prefix and suffix length for the 6rd domain.

Use the **no** form of this command to remove the configuration.

t**unnel 6rd ipv4 prefix-length***prefix-length***suffix-length***suffix-length*

no tunnel 6rd ipv4

Parameter Description

Parameter	Description
prefix-length	The IPv4 prefix length.
suffix-length	The IPv4 suffix length.

Defaults

N/A

Command Mode

Interface configuration mode

Usage Guide

This command is used to configure the common IPv4 prefix and suffix length for the 6rd domain. The valid range is from 0 to 31. The sum of the prefix and suffix lengths is no greater than 31. If this command is not configured, the prefix and suffix lengths are 0 by default.

Configuration Examples

The following example configuresthe IPv4 prefix and suffix length for the 6rd domain of tunnel 100.

```
FS# configureterminal
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is not supported on switches.

6.10 tunnel 6rd prefix

Use this command to configure IPv6 prefix for the 6rd domain.

Use the **no** form of this command to restore the default setting.

tunnel 6rd prefix*ipv6-prefix prefix-length*

no tunnel 6rd prefix

Parameter Description

Parameter	Description
ipv6-prefix	The IPv6 prefix of the 6rd domain.
prefix-length	The IPv6 prefix length of the 6rd domain.

Defaults N/A

Command Mode Interface configuration mode

Usage Guide This command is used to configure the IPv6 prefix for the 6rd domain. This command is mandatory for the 6rd configuration. Without the 6rd prefix, the 6rd tunnel cannot be up. If the prefix length is set to 0, it indicates that the 6rd prefix is removed.

Configuration Examples The following example configuresthe IPv6 prefix for tunnel 100.

```
FS# configureterminal
FS(config)# interface tunnel 100
FS(config-if-Tunnel 100)# tunnel 6rd prefix 2001:da8::/32
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is not supported on switches.

7 FPM Commands

7.1 clear ip fpm counters

Use this command to clear counters about the IPv4 packets.

clear ip fpm counters

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example clears counters about the IPv4 packets.

```
FS# clear ip fpm 1 2 counters
```

Platform Description

N/A

7.2 ip session direct-trans-disable

Use this command to disable the function to transparently transmit packets when the flow table is full.

ip session direct-trans-disable

Use the **no** form of this command to restore the default setting.

no ip session direct-trans-disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This configuration takes effect only on ACs and APs. 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.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration

The following example disables the function to transparently transmit packets when the flow table is full.

Examples

```
FS(config)# ip session direct-trans-disable
```

Platform Description

N/A

7.3 ip session tcp-loose

Use this command to enable the loose TCP status transition check function.

ip session tcp-loose

Use the **no** form of this command to restore the default setting.

no ip session tcp-loose

Parameter Description

Parameter	Description
N/A	N/A.

Defaults

By default, the loose TCP status check function is disabled on FW products while enabled on wireless and EG products.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Platform Description

N/A

7.4 ip session tcp-state-inspection-disable

Use this command to disable the TCP status tracing function.

ip session tcp-state-inspection-disable

Use the **no** form of this command to restore the default setting.

no ip session tcp-state-inspection-disable

Parameter Description

Parameter	Description

Defaults

The TCP status tracing function is enabled on EG and FW products by default.

Command

Global configuration mode

Mode

Usage Guide N/A

Configuration Examples

Platform Description N/A

7.5 ip session tcp-state-inspection-enable

Use this command to enable the TCP status tracing function.

ip session tcp-state-inspection- enable

Use the **no** form of this command to restore the default setting.

no ip session tcp-state-inspection- enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The TCP status tracing function is disabled on ACs and APs by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the TCP status tracing function.

```
FS(config)# ip session tcp-state-inspection-enable
```

Platform Description N/A

7.6 ip session threshold

Use this command to configure the number of packets that can be received for each flow in a certain status.

ip session threshold {**icmp-closed** | **icmp-started** | **rawip-closed** | **tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed**} { *num* }

Use the **no** form of this command to restore the default setting.

no ip sessio threshold {**icmp-closed | icmp-started** | **rawip-closed | tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed**}

Parameter Description

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 5 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.

Defaults

icmp-closed: 10;
icmp-started: 300;
rawip-closed: 10;
tcp-syn-sent: 10;
tcp-syn-receive: 20;
tcp-closed: 20;
udp-closed: 10.

Command Mode

Global configuration mode

Usage Guide

To activate this configuration, run the **ip session track-state-strictly** command.

Configuration Examples

The following example configures the number of packets that can be received for each flow in a certain status to 100.

```
FS(config)# ip session 1 2 threshold tcp-closed 100
```

Platform Description

N/A

7.7 ip session timeout

Use this command to configure the aging time.

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* }

Use the **no** form of this command to restore the default setting.

no 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**}

Parameter Description

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 TCP 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-wait1 status, 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-wait2 status, which is 60 seconds by default and ranges from 10 to 120.
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-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-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

icmp-closed: 10 seconds;

icmp-connected: 10 seconds;

icmp-started: 10 seconds;

rawip-closed: 10 seconds;

rawip-connected; 300 seconds;

rawip-established: 300 seconds;

rawip-started: 300 seconds;

tcp-close-wait: 60 seconds;

tcp-closed: 10 seconds;

tcp-established: 1,800 seconds;

tcp-fin-wait1: 60 seconds;

tcp-fin-wait2: 60 seconds;

tcp-syn-receive: 10 seconds;

tcp-syn-sent: 10 seconds;

tcp-syn_sent2: 10 seconds;

tcp-time-wait: 10 seconds;

udp-closed: 10 seconds;

udp-connected: 30 seconds;

udp-established: 600 seconds;

udp-started: 10 seconds

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the aging time of TCP flows in tcp-established status to 600 seconds.

```
FS(config)# ip session 1 2 timeout tcp-established 600
```

Platform Description

N/A

7.8 ip session track-state-strictly

Use this command to configure packet threshold check for flows in various states.

ip session track-state-strictly

Use the **no** form of this command to restore the default setting.

no ip session track-state-strictly

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

Platform Description N/A

7.9 show ip fpm counters

Use this command to displays the counters about the IPv4 packets.

show ip fpm counters

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the counters about the IPv4 packets, including information about packet loss and flows.

Configuration Examples

Platform Description N/A

7.10 show ip fpm flows

Use this command to display IPv4 packet flow information.

show ip fpm flows

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

Platform Description N/A

7.11 show ip fpm flows filter

Use this command to display IPv4 packet flow information except specific IPv4 packet flows.

show ip fpm flows filter *protocol saddr smask daddr dmask*

Parameter Description

Parameter	Description
protocol	IP protocol in the range from 0 to 255.
saddr	Source IP addresses.
smask	Source IP mask in the range from 1 to 32.
daddr	Destination IP addresses.
dmask	Destination IP mask in the range from 1 to 32.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples N/A

Platform Description N/A

7.12 show ip fpm statistics

Use this command to display IPv4 flow statistics.

show ip fpm statistics

Parameter

Parameter	Description

Description

N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays IPv4 flow statistics on the EG device.

```
FS#show ip fpm statistics
The capacity of the flow table:150016.
Active flows num:109.
event count:65,
Fpm attribute is eg.
```

Field Description

Field	Description
The capacity of the flow table	The number of total flow tables.
Active flows num	The number of active flow tables.
event count:65,	The counter for current events.
Fpm attribute is eg	The flow tables are generated based on EG products.

Platform Description

N/A

8 NAT Commands

8.1 address

Use this command to configure the address range of an empty NAT address pool.

Use the **no** form of this command to delete the address range of an address pool.

address *start-ip end-ip* [**match interface** *interface]*

no address *start-ip end-ip* [**match interface** *interface]*

address interface *interface* [**match interface** *interface]*

no address interface *interface* [**match interface** *interface]*

Parameter Description

Parameter	Description
start-ip	Start IP address of an address block
end-ip	End IP address of an address block
interface *interface*	Sets the interface used when NAT has multiple outside interfaces. The addresses defined in a pool use interface addresses and are used when the interface addresses are unknown and will be negotiated. Note that this parameter must be used with the **match interface** *interface* parameter, and the two interfaces must be consistent. Otherwise, NAT may fail.
match interface *interface*	Sets the interface used when NAT has multiple outside interfaces. When the router determines the egress of packets, NAT uses this egress to select an address that matches it from the pool.

Defaults

No address range is defined by default.

Command Mode

NAT address pool configuration mode

Usage Guide

If you need to define multiple address ranges for an address pool, first enter NAT address pool configuration mode, and then define the NAT address ranges. These commands are not supported on aggregate ports.

Configuration Examples

The following example creates a mulnets address pool and defines two address blocks.

```
FS(config)# ip nat pool mulnets netmask 255.255.255.0
FS(config-nat)# address 172.16.10.1 172.16.10.254
FS(config-nat)# address 192.168.100.1 192.168.100.50
```

Related

Command	Description

Commands

ip nat pool	Defines the IP NAT address pool.

Platform Description

N/A

8.2 ip nat

Use this command to perform NAT on an interface.

Use the **no** form of this command to disable NAT on an interface.

ip nat { **inside** | **outside** }

no ip nat { **inside** | **outside** }

Parameter Description

Parameter	Description
inside	Performs NAT on incoming packets.
outside	Performs NAT on outgoing packets.

Defaults

NAT is not enabled by default.

Command Mode

Interface configuration mode

Usage Guide

NAT is performed only when packets are routed between outside and inside interfaces and meet a certain rule. Therefore, at least an inside interface and an outside interface must be configured.

Configuration Examples

The following example dynamically translates the internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

```
FS#configure terminal
FS(config)# interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)# ip address 192.168.12.6 255.255.255.0
FS(config-if-GigabitEthernet 0/0)# ip nat inside
FS(config-if-GigabitEthernet 0/0)# exit
FS(config)# interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
FS(config-if-GigabitEthernet 0/1)# ip nat outside
FS(config-if-GigabitEthernet 0/1)# exit
FS(config)# ip nat pool net200 200.168.12.1 200.168.12.15 netmask 255.255.255.0
FS(config)# ip nat inside source list 1 pool net200
FS(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat inside destination	Enables NAT for the internal destination address.
ip nat inside source	Enables NAT for internal source addresses.

ip nat outside source	Enables NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool.
show ip nat translations	Displays IP NAT entries.

Platform Description

N/A

8.3 ip nat application

Use this command to implement special application of NAT.

Use the **no** form of this command to cancel this special application.

ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** | **src-change** } *ip-addr*

ip nat application source list *list-num* **destination** { **tcp** | **udp** *dest-ip port-num*} { **dest-change** *ip-addr port-num* | **src-change** *ip-addr* }

no ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** | **src-change** } *ip-addr* **no ip nat application source list** *list-num* **destination** { **tcp** | **udp** *dest-ip port-num*} { **dest-change** *ip-addr port-num* | **src-change** *ip-addr* }

Parameter Description

Parameter	**Description**
list-num	Access list of internal local addresses, that is, match criteria of the source addresses of packets
dest-ip	Internal global address match, that is, match criteria of the destination addresses of packets. NAT entries are created only when the destination IP address matches this address and the source IP address matches the previously defined access list.
tcp *dest-ip port-num*	Matches the internal global address and the destination port. NAT entries are created only when the destination address and port of the TCP packet match the criteria defined here and the source address matches the previously defined access list.
udp *dest-ip port-num*	Matches the internal global address and the destination port. NAT entries are created only when the destination address and port of the UDP packet match the criteria defined here and the source address matches the previously defined access list.
dest-change *ip-addr port-num*	Changes the destination address and port of the packet that meets criteria.
src-change *ip-addr*	Changes the source address of the packet that

	meets criteria.

Defaults This rule is not defined by default.

Command Mode Global configuration mode

Usage Guide In some advanced applications of NAT, it is necessary to change the source or destination addresses of some particular IP packets. This command can be used to perform this operation. The following example uses this command to implement the domain name resolution relay service (DNS relay).

Configuration Examples The following example allows the host in the network segment 192.168.1.0 in the internal network to point the DNS server to the IP address 192.168.1.1 of the NAT inside interface. The NAT function of the router forwards the DNS request from the host in the internal network to the true DNS server 202.101.98.55, and forwards the DNS response packet to the host in the internal network. Implement this function with the **ip nat application** command. The semantics is: If there is a UDP packet whose source address meets the criteria of access-list 1, destination address is 192.168.1.1, and destination port is 53, and then change the destination address of this IP packet to 202.101.98.55 and the destination port to 53.

```
FS#configure terminal
FS(config)# interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)# ip nat inside
FS(config-if-GigabitEthernet 0/0)# exit
FS(config)# interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
FS(config-if-GigabitEthernet 0/1)# ip nat outside
FS(config-if-GigabitEthernet 0/1.)# exit
FS(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0
FS(config)# ip nat inside source list 1 pool net200
FS(config)# access-list 1 permit 192.168.12.0 0.0.0.255
FS(config)# ip nat application source list 1 destination udp 192.168.1.1 53 dest-change 202.101.98.55 53
FS(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Related Commands

Command	Description
address	Defines the address block range of an address pool.
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that NAT should be performed on the traffic that passes this interface.
ip nat inside destination	Enables NAT for the internal destination address.

ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enables NAT for external source addresses.
show ip nat translations	Displays IP NAT entries.

Platform Description N/A

8.4 ip nat inside destination

Use this command to enable NAT for the internal destination address.

Use the **no** form of this command to disable NAT for the internal destination address.

ip nat inside destination list *access-list-number* **pool** *pool-name* [**description** *description-text*]

no ip nat inside destination list *access-list-number*

Parameter Description

Parameter	Description
list *access-list-number*	Internal global addresses are defined in the access list. If the external network accesses the address in the access list, the internal global address will be translated into the internal local address defined in the pool. Note that here you should use the extended ACL in the range from 100 to 199 whose destination IP address is a virtual IP address.
pool *pool-name*	A space in the address pool that defines the internal local address. An internal local address will be assigned from this space during destination address translation.
description *description-text*	(Optional) Description, which contains up to 60 characters. By default, there is no description.

Defaults NAT for the internal source address is disabled by default.

Command Mode Global configuration mode

Usage Guide Translation of internal destination addresses can be performed to realize load balance of TCP traffic. When a host in the internal network is overloaded with TCP traffic, multiple hosts may be required to balance the load of TCP traffic. In this case, you can use NAT to realize load balance of TCP traffic. NAT will create a virtual host to provide the TCP service. This virtual host corresponds to multiple real internal hosts. Then, NAT polls and replaces the destination address, so as to distribute the load. However, no change is made to other IP traffic, unless NAT is configured otherwise.

When NAT is configured to realize TCP load balance, the address of the internal network can be either a valid global address or a private network address. However, the address of the virtual host must be a valid global address.

Configuration Examples

The following example configures the internal network to provide a virtual host address 10.10.10.100 externally. The external network uses this address to access the WWW service. The hosts that provide services in the internal LAN are actually two hosts with the addresses 10.10.10.1 and 10.10.10.2. During NAT, load balance is realized in polling mode.

```
FS#configure terminal
FS(config)# interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)# ip address 10.10.10.254 255.255.255.0
FS(config-if-GigabitEthernet 0/0)# ip nat inside
FS(config-if-GigabitEthernet 0/0)# exit
FS(config)# interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
FS(config-if-GigabitEthernet 0/1)# ip nat outside
FS(config-if-GigabitEthernet 0/1)# exit
FS(config)# ip nat pool net10 10.10.10.1 10.10.10.2 prefix-length 24 type rotary
FS(config)# ip nat inside destination list 100 pool net10
FS(config)# access-list 100 permit ip any host 10.10.10.100
```

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that NAT should be performed on the traffic that passes this interface.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enable NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool
show ip nat translations	Displays IP NAT entries.

Platform Description

N/A

8.5 ip nat inside source

Use this command to enable NAT for internal source addresses in interface configuration mode. Use the **no** form of this command to disable static or dynamic NAT.

ip nat inside source list *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**] [**description** *description-text*]
ip nat inside source static *local-ip global-ip* [**match** *interface-type interface-number* | **netmask** *mask*][**permit-inside**] [**description** *description-text*]
ip nat inside source static *local-ip* **interface** *interface-type interface-number* [**permit-inside**]

[**description** *description-text*]

ip nat inside source static { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } *global-ip global-port* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } **interface** *interface-type interface-number global-port* [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp** *local-ip* **port-range** *local-port1 local-port2* | **udp** *local-ip* **port-range** *local-port1 local-port2*} *global-ip* **port-range** *global-port1 global-port2* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp ip-range** *local-ip1 local-ip2 local-port* | **udp ip-range** *local-ip1 local-ip2 local-port*} **ip-range** *global-ip1 global-ip2 global-port* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp ip-range** *local-ip1 local-ip2* **port-range** *local-port1 local-port2* | **udp ip-range** *local-ip1 local-ip2* **port-range** *local-port1 local-port2*} **ip-range** *global-ip1 global-ip2* **port-range** *global-port1 global-port2* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp** *local-ip* **port-range** *local-port1 local-port2* | **udp** *local-ip* **port-range** *local-port1 local-port2*} **interface** *interface-type interface-number* **port-range** *global-port1 global-port2* [**permit-inside**] [**description** *description-text*]

no ip nat inside source list *access-list-number*

no ip nat inside source static *local-ip global-ip*

no ip nat inside source static *local-ip* **interface** *interface-type interface-number*

no ip nat inside source static { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } *global-ip global-port*

no ip nat inside source static { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } **interface** *interface-type interface-number global-port*

Parameter Description

Parameter	Description
list *access-list-number*	Specifies the access list of local addresses. NAT entries will be created only for the traffic with the source address that matches this access list.
interface *interface-type interface-number*	Uses the global address of the outside interface to perform Network Address Port Translation (NAPT), also called extended NAT.
pool *pool-name*	Uses a global address in the address pool to perform NAT.
overload	(Optional) Every global address in the pool can be reused for translation, namely, NAPT. Currently, this parameter is not set, and global addresses are reusable. This parameter is added in

	order to be compatible with the command of Cisco.
static *local-ip global-ip*	Defines the simple static NAT. local-ip is a local address, and global-ip is a global address. The **no** form of this command does not check the validity of global-ip.
static *protocol*	Defines the extended static NAT. protocol can be either TCP or UDP.
local-port	Service port number (TCP or UDP) of the local address. Each service typically corresponds to a service port.
global-port	Service port number of the global address. The external network accesses the services of hosts in the internal network through this port. This port number can be different from local-port.
ip-range *local-ip1 local-ip2*	Specifies an internal IP range. local-ip1 and local-ip2 are start IP address and end IP address respectively.
ip-range *global-ip1 global-ip2*	Specifies an external IP range. local-ip1 and local-ip2 are start IP address and end IP address respectively.
port-range *local-port1 local-port2*	Specifies an internal port range. local-port1 and local-port2 are start port and end port respectively,
port-range *global-port1 global-port2*	Specifies an external port range. local-port1 and local-port2 are start port and end port respectively,
permit-inside	Allows users in the internal network to access the host with the IP address indicated by local-ip through global-ip. This keyword appears only in the **ip nat inside source static** command is applicable only on routers.
match *interface-type interface-number*	Specifies the outside interface (used in smart DNS).
netmask *mask*	Network mask
description *description-text*	Configures a string of up to 60 characters.

Defaults NAT for internal source addresses is disabled by default.

Command Global configuration mode

Mode

Usage Guide

When the IP address of the internal network is a private address and the internal network needs to communicate with the external network, NAT must be configured to translate the internal private IP address into the globally unique IP address.

If organizations, such as net bars or enterprises, access the network only for obtaining resources in the external network, such as browsing Web pages, receiving and sending emails, and downloading files, but not for providing network services for the external network, the IP address of the outside interface can be used directly as the global address and the address is translated in NAPT mode. If NAT is not configured, the internal network with the private address, even if physically interconnected with the external network, is unable to interwork with the external network, because the external network does not provide network routing for the private address.

Static NAT or NAPT should be configured for the internal hosts that provide services. To ensure continuous service provisioning, do not use the address of the outside interface to perform NAPT because this address is interconnected with ISP and is very likely to be translated. Generally, users in the internal network can access the services provided by these internal hosts simply by using the IP address of the internal network. However, some special application services can only be accessed by users in the internal network using the global IP address. In this case, you need to add the keyword **permit-inside** when configuring static NAT or static NAPT for internal source addresses. Moreover, it is advisable to run the **no ip redirects** command on the inside interface to prevent the inside interface from sending redirection packets.

Configuration Examples

The following example dynamically translates the internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

```
FS#configure terminal
FS(config)# interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)# ip address 192.168.12.6 255.255.255.0
FS(config-if-GigabitEthernet 0/0)# ip nat inside
FS(config-if-GigabitEthernet 0/0)# exit
FS(config)# interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
FS(config-if-GigabitEthernet 0/1)# ip nat outside
FS(config-if-GigabitEthernet 0/1)# exit
FS(config)# ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28
FS(config)# ip nat inside source list 1 pool net200
FS(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that the NAT should be performed on the traffic that passes this

	interface.
ip nat inside destination	Enables NAT for the inside destination address.
ip nat outside source	Enable NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool.
show ip nat translations	Displays IP NAT entries.

Platform Description N/A

8.6 ip nat keepalive

Use this command to configure the interval of sending gratuitous ARP (GARP) packets with the local address.

ip nat keepalive [*keealive_out*]

no ip nat keepalive

default ip nat keepalive

Parameter Description

Parameter	Description
keealive_out	Sending interval

Defaults The interval of sending GARP packets with the local address is not configured by default.

Command Mode Global configuration mode

Usage Guide Some addresses in NAT rules should be taken as the local address. Sending GARP packets at intervals avoids address conflicts.

Configuration Examples The following example sets the interval of sending GARP packets with the local address to 10 seconds.

```
FS#configure terminal
FS(config)# ip nat keepalive 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.7 ip nat outside source

Use this command to enable NAT for the external source addresses.

Use the **no** form of this command is used to disable NAT for external source addresses.

ip nat outside source list *access-list-number* **pool** *pool-name*

ip nat outside source static *global-ip local-ip*

ip nat outside source static { **tcp** *global-ip global-port* | **udp** *global-ip global-port* } *local-ip local-port*

no ip nat outside source list *access-list-number*

no ip nat outside source static *global-ip local-ip*

no ip nat outside source static { **tcp** *global-ip global-port* | **udp** *global-ip global-port* } *local-ip local-port*

Parameter Description

Parameter	Description
list *access-list-number*	Global address access list. NAT entries will be created only for the traffic with the source address that matches this access list.
pool *pool-name*	Uses a local address in the address pool to perform NAT.
static *global-ip local-ip*	Defines the simple static NAT. *local-ip* is a local address, and *global-ip* is a global address.
static *protocol*	Defines the extended static NAT. *protocol* can be either TCP or UDP.
local-port	Service port number (TCP or UDP) of the local address. Each service typically corresponds to a service port. This port number can be different from *global-port*.
global-port	Service port number of the global address

Defaults NAT for external source addresses is disabled by default.

Command Mode Global configuration mode

Usage Guide NAT for external source addresses is mainly used for the overlapped address space. Two private networks to be interconnected are assigned with the same IP address, or a private network and a public network are assigned with the same global IP address, which is called address overlap. Two network hosts with the overlapped address cannot communicate with each other because they both determine that the remote host is located in the local network. Overlapped address NAT is configured to resolve the problem of communication between networks with the overlapped address. With overlapped address NAT configured, the external network host address behaves like another network host address in the internal network, and vice versa.

Configuration of overlapped address NAT includes two steps: 1) Configure the internal source address NAT; 2) Configure the external source address NAT. The external source address translation can be configured only when the address of the external network is overlapped with that of the internal network. The external source address translation can be configured as static NAT or dynamic NAT.

Address overlap is inevitable when a non-registered global IP address is assigned to connect to the Internet during internal network construction. Because the internal network generally uses the domain name to access the external network host, routers must support NAT for DNS packets.

Configuration Examples

In the following example, the address of the internal network 92.168.12.0/24 is overlapped with that of the external network. After translation, the internal host can access the host in the network segment 92.168.12.0/24 in the external network through the network address 192.168.12.0/24.

```
FS#configure terminal
FS(config)# interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)# ip address 192.168.12.55 255.255.255.0
FS(config-if-GigabitEthernet 0/0)# ip nat inside
FS(config-if-GigabitEthernet 0/0)# exit
FS(config)# interface Serial 10/1
FS(config-if-GigabitEthernet 0/1)# ip address 192.168.10.1 255.255.255.0
FS(config-if-GigabitEthernet 0/1)# ip nat outside
FS(config-if-GigabitEthernet 0/1)# encapsulation ppp
FS(config-if-GigabitEthernet 0/1)# exit
FS(config)#ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28
FS(config)#ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24
FS(config)#ip nat inside source list   1 pool net200
FS(config)#ip nat outside source list 1 pool net192
FS(config)#access-list 1 permit 92.168.12.0 0.0.0.255
FS(config)#ip route 192.168.12.0 255.255.255.0 192.168.100.2
```

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that NAT should be performed for the traffic that passes this interface.
ip nat inside destination	Enables NAT for internal destination address.
ip nat inside source	Enables NAT for internal source address.
ip nat pool	Defines the IP NAT address pool.
show ip nat translations	Displays IP NAT entries.

Platform Description

N/A

8.8 ip nat pool

Use this command to define an address pool for NAT.

Use the **no** form of this command to delete the address pool.

ip nat pool *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]

ip nat pool *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]

ip nat pool *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**] [**hardware**]

no ip nat pool *pool-name*

Parameter Description

Parameter	Description
pool-name	Name of the NAT address pool
start-ip	Start IP address of the NAT address pool
end-ip	End IP address of the NAT address pool
netmask *netmask*	Net mask of an address in the NAT address pool
prefix-length *prefix-length*	Length of the net mask of an address in the NAT address pool
type	Type of the NAT address pool. **rotary** means round robin. That is, each address has the same probability of being assigned. The type is **rotary** no matter whether **rotary** is set. The **rotary** parameter is introduced in order to keep compatible with the command of Cisco.
hardware	(NPE80) Hardware-based address pool. NAT of this type is handled by hardware with a higher connection speed.

Defaults

No address pool is defined by default.

Command Mode

Global configuration mode

Usage Guide

If multiple address blocks must be defined for an address pool, first create an empty address pool, and define the address range.

Configuration Examples

The following example creates an address pool named **net192**, with the start address 192.168.12.1, end address 192.168.12.254, and a 24-bit net mask.

```
FS#configure terminal
FS(config)# ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24
```

Related

Command	Description

Commands

address	Defines the address block range of an address pool.
clear ip nat translation	Clears the NAT entry table.
ip nat	Specifies that NAT should be performed for the traffic that passes this interface.
ip nat inside destination	Enables NAT for inside destination addresses.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enables NAT for external source addresses.
show ip nat statistics	Displays IP NAT statistics.
show ip nat translations	Displays IP NAT entries.

Platform Description N/A

8.9 ip nat translation

Use this command to configure the NAT Application Layer Gateway (ALG).

ip nat translation { **dns** [**ttl** *ttl_time*] **| ftp** [**port** *port_num*] **| tftp | pptp | h323 | rtsp | sip** }

no ip nat translation { **dns | ftp | tftp | pptp | h323 | rtsp | sip** }

Parameter Description

Parameter	Description
ttl_time	Defines the UDP TTL for DNS. The default is 0.
port_num	Defines the port for FTP. The default is 21.

Defaults All NAT ALGs are enabled by default.

Command Mode Global configuration mode

Usage Guide In NAT application, the IP addresses and ports of data packets are changed. However, the IP addresses and ports of certain special protocols are contained in the valid data of the application layer. To successfully perform NAT for such special protocols, the specific protocol gateway needs to be enabled.

Configuration Examples

The following example configures DNS TTL to 30 seconds.

```
FS#configure terminal
FS(config)# ip nat translation dns ttl 30
```

The following example configures Port 25 for FTP.

```
FS#configure terminal
```

```
FS(config)# ip nat translation ftp port 25
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.10 show ip nat translations

Use this command to display NAT translations.

show ip nat translations [*acl_num*] [**icmp** | **tcp** | **udp**] [**verbose**]

Parameter Description

Parameter	Description
icmp	Displays NAT entries only for ICMP.
tcp	Displays NAT entries only for TCP.
udp	Displays NAT entries only for UDP.
acl_num	ACL number, which supports only the extended ACL to filter the displayed content.
verbose	Displays more detailed NAT entries.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command can be used to display the summary of IP NAT entries, such as protocols, internal global addresses and port numbers, internal local addresses and port numbers, external local addresses and port numbers, and external global addresses and port numbers. Used with the **verbose** parameter, it displays more detailed information, including the timeout period configured for each entry, remaining time for this entry, and flag of the entry.

Configuration Examples

The following example displays NAT translations.

```
FS# show ip nat translations verbose
timeout for NAT TCP flows: 86400
timeout for NAT TCP flows after a FIN or RST: 60
timeout for NAT TCP flows after a SYN : 60
timeout for NAT UDP flows: 300
timeout for NAT DNS flows: 60
timeout for NAT ICMP flows: 60
Pro Inside global          Inside local          Outside local          Outside global timeout vrf
tcp   192.168.5.103:1987   192.168.211.21   :1987   211.67.71.7          :80          211.67.71.7:80
```

```
timeout=85139 1
udp 192.168.5.103:1041 192.168.211.183:1041 202.101.98.55    :53 202.101.98.55:53 timeout=38
1
```

Field Description

Field	Description
Pro	Protocol type. **udp** indicates the UDP translation entry. **tcp** indicates the TCP entry. **icmp** indicates the ICMP translation entry.
Inside global	Internal global address and port number
Inside local	Internal local address and port number
Outside local	External local address and port number
Outside global	External global address and port number
timeout	Time (in seconds) left before this NAT entry times out
vrf	VRF where the connection is

Related Commands

Command	Description
clear ip nat translation	Clears the NAT entry table.
ip nat	Performs NAT on the traffic that passes this interface.
ip nat inside destination	Enables NAT for internal destination addresses.
ip nat inside source	Enables NAT for internal source addresses.
ip nat outside source	Enables NAT for external source addresses.
ip nat pool	Defines the IP NAT address pool.
show ip nat translations	Displays IP NAT entries.

Platform Description

N/A

9 MLLB Commands

9.1 load-monitor uplink

Use this command to configure uplink load monitoring of MLLB.

load-monitor uplink

Use the **no** form of this command to cancel uplink load monitoring of MLLB.

no load-monitor

Use this command to restore the default configuration.

default load-monitor

Parameter Description

Parameter	Description
N/A	N/A

Defaults Downlink load is monitored by default.

Command Mode Global configuration mode

Usage Guide Generally, the downlink traffic of an egress interface is greater than the uplink traffic. In some scenarios, for example, a scenario with a LAN server, the uplink traffic may be greater than the downlink traffic. In this case, the uplink traffic can be monitored to calculate the bandwidth utilization rate and threshold.

Configuration Example #Configure uplink load monitoring of MLLB.

```
FS(config)#load-monitor uplink
```

#Cancel uplink load monitoring of MLLB.

```
FS(config)#no load-monitor
```

Verification Run the **show mllb configure** command to display the configuration information of MLLB.

9.2 mllb detect domain add

Use this command to add domain names to be detected by MLLB.

mllb detect domain add *domain-name*

Use the **no** form of this command to delete all domain names detected by MLLB.

no mllb detect domain add

Use the **no** form of this command to delete specified domain names detected by MLLB.

no mllb detect domain add *domain-name*

Parameter Description

Parameter	Description
domain-name	Indicates a domain name. A domain name contains no more than 63 characters.

Defaults No domain name is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to add a domain name to be detected.

Configuration Example #Add a domain name to be detected by MLLB.

FS(config)#mllb detect domain add www.baidu.com

#Delete a domain name detected by MLLB.

FS(config)#no mllb detect domain add www.baidu.com

Verification Run the **show mllb detect configure** command to display added domain names.

9.3 mllb detect domain dns-server

Use this command to add DNS servers and interfaces to be detected by MLLB.

mllb detect domain dns-server *dns-ip interface* [**source-ip** *src-ip*]

Use the **no** form of this command to delete all DNS servers and interfaces detected by MLLB.

no mllb detect domain dns-server

Use the **no** form of this command to delete specified DNS servers and interface detected by MLLB.

no mllb detect domain dns-server *dns-ip interface*

Parameter Description

Parameter	Description
dns-ip	Indicates the IP address of a DNS server and the type of the IP address.
interface	Indicates the name of an interface.
src-ip	Specifies the source IP address of a detection packet.

Defaults No IP address or interface of a DNS server is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to add a DNS server to be detected.

Configuration Example

#Add a DNS server, interface, and source IP address to be detected.

```
FS(config)#mllb detect domain dns-server 114.114.114.114 GigabitEthernet 0/4 source-ip 192.168.197.16
```

#Delete a DNS server and interface detected by MLLB.

```
FS(config)#no mllb detect domain dns-server 114.114.114.114 GigabitEthernet 0/4
```

Verification

Run the **show mllb detect configure** command to display added DNS servers.

9.4 mllb detect domain enable

Use this command to enable domain name detection and detect the accessibility of domain names by polling according to the set period.

mllb detect domain enable

Use the **no** form of this command to disable domain name detection.

no mllb detect domain enable

Use this command to restore the default configuration.

default mllb detect domain enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Domain name detection is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable domain name detection.

Configuration Example

#Enable domain name detection.

```
FS(config)#mllb detect domain enable
```

#Disable domain name detection and the database recording function.

```
FS(config)#no mllb detect domain enable
```

Verification

Run the **show mllb detect configure** command to display the status of domain name detection.

1. If domain name detection is enabled, the following message is displayed:

```
FS(config)#mllb detect domain enable
mllb detect domain is enabled.
```

2. If domain name detection is disabled, the following message is displayed:

```
FS(config)#no mllb detect domain enable
mllb detect domain is disabled!
```

9.5 mllb detect domain interval

Use this command to configure the domain name detection interval.

mllb detect domain interval *interval-time*

Use the **no** form of this command to cancel the domain name detection interval.

no mllb detect domain interval

Use this command to restore the default configuration.

default mllb detect domain interval

Parameter Description

Parameter	Description
interval-time	Indicates a domain name detection interval in minutes. The value range is from 1 to 1,440.

Defaults The domain name detection interval is five minutes by default.

Command Mode Global configuration mode

Usage Guide The domain name detection function is performed on a regular basis according to the configured domain name, DNS server, and egress interface. Use this command to change the detection interval.

ⓘ The detection interval is subject to the detection duration and is not an absolute value. Though the default detection interval is five minutes, the second detection will be performed at a time later than the five-minute interval, instead of at the exact time point of the five-minute interval.

Configuration Example

#Set the domain name detection interval to 10 minutes.

```
FS(config)#mllb detect domain interval 10
```

#Cancel the domain name detection interval.

```
FS(config)#no mllb detect domain interval
```

Verification Run the **show mllb detect configure** command to display the configuration information of domain name detection.

9.6 mllb detect network enable

Use this command to enable network detection, detect networks by polling according to the set period, and record detected networks into the database.

mllb detect network enable

Use the no form of this command to disable network detection.

no mllb detect network enable

Use this command to restore the default configuration.

default mllb detect network enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Network detection and database recording are disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable network detection and record detected networks into databases.

After the function is enabled, network delay, including TCP and UDP packet delays, will be detected regularly, and the number of half-open connections (response packets are not received) and traffic values of different routing modules are measured.

Configuration Example

```
#Enable network detection.
FS(config)#mllb detect network enable

#Disable network detection.
FS(config)#no mllb detect network enable
```

Verification Run the **show mllb detect** configure command to display the status of network detection.

9.7 mllb detect network interval

Use this command to configure a network detection interval.

mllb detect network interval *interval-time*

Use the **no** form of this command to cancel the network detection interval.

no mllb detect network interval

Use this command to restore the default configuration.

default mllb detect network interval

Parameter Description

Parameter	Description
interval-time	Indicates a network detection interval in minutes. The value range is from 1 to 1,440.

Defaults The network detection interval is five minutes by default.

Command Mode Global configuration mode

Usage Guide The network detection function is performed at an interval of five minutes. Use this command to change the detection interval.

Configuration Example

#Set the network detection interval to 10 minutes.

```
FS(config)#mllb detect network interval 10
```

#Restore the network detection interval.

```
FS(config)#no mllb detect network interval
```

Verification

Run the **show mllb detect configure** command to display the configuration information of network detection.

9.8 mllb enable

Use this command to enable MLLB.

mllb enable

Use the **no** form of this command to disable MLLB.

no mllb enable

Use this command to restore the default configuration.

default mllb enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

MLLB is disabled by default.

Command Mode

Global configuration mode

Usage Guide

To enable the gateway to support load balancing, enable MLLB.

⚠ The load balancing function of MLLB is applicable to ECMP egress interfaces only.

Configuration Example

#Enable MLLB.

```
FS(config)# mllb enable
```

#Disable MLLB.

```
FS(config)#no mllb enable
```

Verification

Run the **show mllb configure** command to display the status of MLLB.

9.9 mllb first-choice

Use this command to configure the preferred egress interface of MLLB.

mllb first-choice *interface-type interface-number*

Use the **no** form of this command to cancel the preferred egress interface of MLLB.

no mllb first-choice

Use this command to restore the default configuration.

default mllb first-choice

Parameter Description

Parameter	Description
interface-type interface-number	Indicates the name of an interface.

Defaults No preferred egress interface is configured by default.

Command Mode Global configuration mode

Usage Guide If the load of any one egress interface exceeds the threshold, no interface can balance load based on the predefined policy. In this case, use this command to configure a preferred egress interface.

ℹ This command applies to ECMP egress interfaces of default routes only.

Configuration Example #Configure GigabitEthernet 0/1 as a preferred egress interface.

```
FS(config)# mllb first-choice GigabitEthernet 0/1
```

Verification Run the **show mllb configure** command to display the configuration information of MLLB.

9.10 mllb interface

Use this command to configure the weight of an MLLB interfaces.

mllb interface *inteface* **weight** *weight-num*

Use the **no** form of this command to delete the weights of an MLLB interface.

no mllb interface *inteface* **weight**

Use this command to restore the default weight of an MLLB interface.

default mllb interface *inteface* **weight**

Parameter Description

Parameter	Description
Interface	Indicates the name of an interface.
weight-num	Specifies a weight value in kbps. The value range is from 1 to 40,000,000.

Defaults The weight value of an interface is the downlink bandwidth by default.

Command Mode Global configuration mode

Usage Guide The weight value of an interface is the downlink bandwidth by default. Use this command to specify the weight value of a specified interface in order to change the bandwidth utilization of the interface. For example, the downlink bandwidth of the GE0/4 interface is 100 Mbps and the default weight value is 100,000 kbps. To increase the bandwidth utilization of the interface, change the weight value to 150,000 kbps; to decrease the bandwidth utilization of the interface, change the weight value to 50,000 kbps.

Configuration Example

#Set the weight value of the GE0/4 interface to 100 Mbps.

```
FS(config)#mllb interface GigabitEthernet 0/4 weight 100000
```

#Restore the weight value to the default downlink bandwidth of the interface.

```
FS(config)#no mllb interface GigabitEthernet 0/4 weight
```

Verification Run the **show run | include mllb** command to display the weight value of the specified MLLB interface.

1. If the weight value of the GE0/4 interface is 100 Mbps, the following message is displayed:

```
FS(config)# mllb interface GigabitEthernet 0/4 weight 100000
mllb interface GigabitEthernet 0/4 weight set to 100000.
```

2. If the weight value of the GE0/4 interface is restored, the following message is displayed:

```
FS(config)#no mllb interface GigabitEthernet 0/4 weight 100000
clear mllb interface GigabitEthernet 0/4 weight!
```

9.11 mllb load-interval

Use this command to configure the load update period of MLLB.

mllb load-interval *refresh-time*

Use the **no** form of this command to cancel the load update period of MLLB.

no mllb load- interval

Use this command to restore the default configuration.

default mllb load- interval

Parameter Description

Parameter	Description
refresh-time	Indicates an update period in seconds. The value range is from 3 to 30.

Defaults Load is updated at an interval of five seconds by default.

Command Mode Global configuration mode

Usage Guide

By default, MLLB calculates interface load at an interval of five seconds, and determines whether the load exceeds a threshold. Use this command to change the default value.

Configuration Example

#Set the load update period of MLLB to 10 seconds.

```
FS(config)#mllb load-interval 10
```

#Cancel the load update period of MLLB.

```
FS(config)#no mllb load-interval
```

Verification

Run the **show mllb configure** command to display the configuration information of MLLB.

9.12 mllb load-sharing original

Use this command to balance load based on the source IP address. This command applies to bandwidth-based policies only. Packets with the same source IP address are transmitted through the same egress interface.

mllb load-sharing original

Use the **no** form of this command to cancel the configuration.

no mllb load-sharing

Use this command to restore the default configuration.

default mllb load-sharing

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Packets are sent based on the source and destination IP addresses by default.

Command Mode

Global configuration mode

Usage Guide

Packets of some applications may be distributed to multiple egress interfaces according to the source and destination IP addresses, which causes reconnection and intermittent interruption. These problems can be resolved if packets are distributed according to the source IP address only.

Configuration Example

#Balance load based on the source IP address.

```
FS(config)#mllb load-sharing original
```

#Cancel the configuration.

```
FS(config)#no mllb load-sharing
```

Verification

Run the **show mllb configure** command to display the configuration information of MLLB.

9.13 mllb policy

Use this command to configure a load balancing policy of MLLB.

mllb policy {**bandwidth** | **load**}

Use the **no** form of this command to cancel the load balancing policy of MLLB.

no mllb policy

Use this command to restore the default configuration.

default mllb policy

Parameter Description

Parameter	Description
N/A	N/A

Defaults MLLB balances load based on the bandwidth by default.

Command Mode Global configuration mode

Usage Guide

⚠ If the bandwidth-based policy is enabled, the bandwidth of the egress interface must be configured.

Configuration Example

#Configure the bandwidth-based policy of MLLB.

```
FS(config)# mllb policy bandwidth
```

#Configure the load-based policy of MLLB.

```
FS(config)# mllb policy load
```

Verification Run the **show mllb configure** command to display the configuration information of MLLB.

9.14 mllb threshold

Use this command to configure load thresholds of MLLB.

mllb threshold { *percent-upper* | [**lower** *percent-lower*] }

Use the **no** form of this command to restore the load thresholds of MLLB.

no mllb threshold

Use this command to restore the default configurations.

default mllb threshold

Parameter Description

Parameter	Description
threshold *percent-upper*	Indicates an upper threshold in percentage. The value range is from 1 to 100.

lower *percent-lower*	Indicates a lower threshold in percentage. The value range is from 1 to 100.

Defaults

The upper and lower thresholds of egress interfaces are 100, respectively.

Command Mode

Global configuration mode

Usage Guide

Use 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 threshold, the link will not be selected for load balancing. If the load of the link becomes smaller than a lower threshold, the link is selected to balance load. Load thresholds are indicated by percentage, and the value range is from 1 to 100. The lower threshold is smaller than or equal to the upper threshold.

Configuration Example

#Set the upper threshold to 95% and lower threshold to 85%.

```
FS(config)#mllb threshold 95 lower 85
```

#Set the upper threshold to 95%.

```
FS(config)#mllb threshold 95
```

#Set the lower threshold to 85%.

```
FS(config)#mllb threshold lower 85
```

Verification

Run the **show mllb configure** command to display the configuration information of MLLB.

9.15 show mllb configure

Use this command to display MLLB configuration information.

show mllb configure

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to display MLLB configuration information.

Configuration Example

#Display MLLB configuration information.

```
FS#show mllb configure
multi-link load balance configure:
multi-link load balance state: enable
multi-link load balance policy: load
multi-link load balance load-interval: 5
multi-link load balance threshold: 90 lower: 90
```

```
multi-link load balance load-monitor: down-link
multi-link load balance first-choice set to GigabitEthernet 0/1 is up
multi-link load balance load-sharing no original
```

Field description:

Field	Description
state	Indicates the MLLB state.
policy	Indicates a load balancing policy of MLLB.
load -interval	Indicates a load update interval.
threshold	Indicates an upper load threshold.
lower	Indicates a lower load threshold.
load-monitor	Indicates a load monitoring direction.
first-choice	Prioritizes an egress interface.
load-sharing	Indicates a source IP address.

9.16 show mllb detect configure

Use this command to display MLLB detection configuration information.

show mllb detect configure

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to display MLLB detection configuration information.

Configuration Example

#Display MLLB detection configuration information.

```
FS#show mllb detect configure
mllb detect configure:
network detect state: true
network detect interval: 300 seconds
domain detect state: true
domain detect interval: 300 seconds
domain detect name:
    domain name: www.cqu.edu.cn
    domain name: www.baidu.com
    total domain number: 2
  domain detect dns server:
    dns server and interface: 114.114.114.114 GigabitEthernet 0/4 source-ip 192.168.197.16
    dns server and interface: 192.168.58.110 GigabitEthernet 0/4
    total dns server and interface number: 2
has storage: true
```

Field description:

Field	Description
state	Indicates the states of network detection and domain name detection.
interval	Indicates the intervals of network detection and domain name detection.
name	Indicates a domain name to be detected.
dns server	Indicates the DNS server and interface to be detected.
domain number	Indicates the number of configured domain names.
interface number	Indicates the number of configured DNS servers (interfaces).
storage	Indicates a storage device. If no storage device exists, the detection result will not be recorded into the database.

9.17 database from

Use this command to display information about the domain name database detected by MLLB.

show mllb detect domain database from *begin-year begin-month begin-day begin-hour* [**to** *end-year end-month end-day end-hour*]

Parameter Description

Parameter	Description
begin-year	Indicates the start year of a period.
begin-month	Indicates the start month of a period.
begin-day	Indicates the start day of a period.
begin-hour	Indicates the start time of a period.
end-year	Indicates the end year of a period.
end-month	Indicates the end month of a period.
end-day	Indicates the end day of a period.
end-hour	Indicates the end time of a period.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide Use this command to display information about the domain name database detected by MLLB.

Configuration Example #Display information about the domain name database detected by the MLLB.

```
FS#show mllb detect domain database from 2016 1 21 0:0:0
Date & Time                 Domain                              Dns-server            Ifindex     Parse-ip
Dns-time     Tcp-connect       Http_get
2016-01-21  00:00:07              www.cqu.edu.cn                                 192.168.58.110               5
222.178.10.35               1              65                     59/1
2016-01-21  00:00:07              www.baidu.com                                  192.168.58.110               5
```

```
115.239.211.112          1              23                   25/1
2016-01-21  00:00:07              www.gov.cn                                              192.168.58.110                5
117.26.144.16            0              18                   197/1
```

Field description:

Field	Description
Date & Time	Indicates the date and time of domain name detection.
Domain	Indicates a domain name to be detected.
Dns-server	Indicates the IP address of a configured DNS server.
Ifindex	Specifies the index of an egress interface.
Parse-ip	Indicates the IP address parsed out from the domain name.
Dns-time	Indicates DNS parsing duration in milliseconds.
Tcp-connect	Indicates TCP connection duration in milliseconds.
Http_get	Indicates HTTP Get request duration in milliseconds. The value **1** indicates request success, and the value **0** indicates a request exception.

9.18 show mllb detect domain database select

Use this command to display specified information about the domain name database detected by MLLB.

show mllb detect domain database select { **dns-server** *dns-ip* **| domain** domain-name **| error | interface** *interface* } { **error from | from**} *begin-year begin-month begin-day begin-hour* [**to** *end-year end-month end-day end-hour*]

Parameter Description

Parameter	Description
dns-ip	Indicates the IP address of a DNS server.
domain-name	Indicates a domain name.
interface	Indicates the name of an interface.
begin-year	Indicates the start year of a period.
begin-month	Indicates the start month of a period.
begin-day	Indicates the start day of a period.
begin-hour	Indicates the start time of a period.
end-year	Indicates the end year of a period.
end-month	Indicates the end month of a period.
end-day	Indicates the end day of a period.
end-hour	Indicates the end time of a period.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to display specified information about the domain name database detected by MLLB.

Configuration Example

#Display information about failures in detecting domain name databases by MLLB.

```
FS#show mllb detect domain database select error from 2016 1 21 0:0:0
Date & Time                  Domain                             Dns-server              Ifindex      Parse-ip
```

```
Dns-time      Tcp-connect          Http_get
2016-01-21  00:00:39                  www.baidu.com                                              114.114.114.114               5
115.239.210.27             33              0                        0/0
2016-01-21  00:01:44                  www.baidu.com                                              114.114.114.114               5
115.239.210.27             22              0                        0/0
2016-01-21  00:03:20                  www.baidu.com                                              192.168.58.110                5
115.239.210.27             0               0                        0/0
```

Field description:

Field	Description
Date & Time	Indicates the date and time of domain name detection.
Domain	Indicates a domain name to be detected.
Dns-server	Indicates the IP address of a configured DNS server.
Ifindex	Specifies the index of an egress interface.
Parse-ip	Indicates the IP address parsed out from the domain name. The value 0.0.0.0 indicates a parsing failure.
Dns-time	Indicates DNS parsing duration in milliseconds.
Tcp-connect	Indicates TCP connection duration in milliseconds. The value 0 indicates a connection failure.
Http_get	Indicates HTTP Get request duration in milliseconds. The value **1** indicates request success, and the value **0** indicates a request exception.

9.19 show mllb detect domain name

Use this command to display information about a specified domain name to be detected by MLLB.

show mllb detect domain name *domain-name dns-ip* [*interface* [**source-ip** *src-ip*]]

Parameter Description

Parameter	Description
domain-name	Indicates a domain name to be detected.
dns-ip	Parses the domain name from this DNS server.
interface	Detects the interface for performing domain name detection.
src-ip	Specifies the source IP address of a detection packet.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to display information about a specified domain name to be detected by MLLB.

Configuration Example

#Display information about a specified domain name to be detected by MLLB.

```
FS#show mllb detect domain name www.qq.com 114.114.114.114 gigabitEthernet 0/4 source-ip 192.168.197.16
Input parameter: domain www.qq.com, dns server ip 114.114.114.114, out interface GigabitEthernet 0/4.
Output:
  dns parse ok: true.
```

```
tcp connect ok: true.
http get ok: true.
dns parse ip: 140.206.160.207.
dns parse delay: 24ms, tcp connect delay: 21ms, http get delay: 21ms.
```

Field description:

Field	Description
dns parse ok	Indicates whether a domain name is successfully parsed.
tcp connect ok	Indicates whether a TCP connection is successfully established.
http get ok	Indicates whether an HTTP Get request is responded to.
dns parse ip	Indicates the first IP address parsed out from the domain name by the DNS server.
delay	Indicates delays in milliseconds, which successively include the DNS parsing delay, TCP connection delay, and HTTP Get request delay.

9.20 show mllb detect network

Use this command to display information about a network detected by MLLB.

show mllb detect network {**interface** [*interface-name*] **|** *source-ip source-ip-mask destination-ip destination-ip-mask* **|** **database** {**select interface** *select-interface-name* **from | from**}} *begin-year begin-month begin-day begin-hour* [**to** *end-year end-month end-day end-hour*]

Parameter Description

Parameter	Description
interface-name	Specifies the name of an interface of a detected network.
source-ip	Specifies the source IP address of a detected network.
source-ip-mask	Specifies the source IP mask of a detected network.
destination-ip	Specifies the destination IP address of a detected network.
destination-ip-mask	Specifies the destination IP mask of a detected network.
select-interface-name	Displays information about a specified interface of the database of a detected network.
begin-year	Indicates the start year of a period.
begin-month	Indicates the start month of a period.
begin-day	Indicates the start day of a period.
begin-hour	Indicates the start time of a period.
end-year	Indicates the end year of a period.
end-month	Indicates the end month of a period.
end-day	Indicates the end day of a period.
end-hour	Indicates the end time of a period.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide Use this command to display information about a network detected by MLLB.

Configuration Example #Display information about a network detected by MLLB.

```
FS#show mllb detect network interface

The analysis of half connection:
   Interface                                   Half(ALL total)      Half(TCP total)      Half(UDP total)      Half(DNS total)
   GigabitEthernet 0/4                        2/11                      0/7                        2/4                        0/0
   GigabitEthernet 0/5                        0/1                       0/0                        0/0                        0/0

The analysis of delay:
   Interface                                          Total delay(Min/Aver/Max/Count)        TCP delay(Min/Aver/Max/Count)
UDP delay(Min/Aver/Max/Count)           DNS delay(Min/Aver/Max/Count)
   GigabitEthernet  0/4                                 0/35/180/9                                                   0/15/60/7
0/105/180/2                                    0/0/0/0
   GigabitEthernet  0/5                                 0/0/0/0                                                        0/0/0/0
0/0/0/0                                        0/0/0/0

The analysis of route flows:
   Interface                                                             Route   type                    Total(Output/Input)Mbit
TCP(Output/Input)                          UDP(Output/Input)                           DNS(Output/Input)
   GigabitEthernet 0/4                         ref_ip                  64/168                                              64/160
0/0                                          0/0
   GigabitEthernet 0/5                          ref_ip                  0/0                                                    0/0
0/0                                          0/0
FS#
```

Field description:

Field	Description
Interface	Indicates the name of a detected interface.
Half(ALL total)	Indicates the number of half-open connections and total number of connections of all protocols.
Half(TCP total)	Indicates the number of half-open TCP connections and total number of TCP connections.
Half(UDP total)	Indicates the number of half-open UDP connections and total number of UDP connections.
Half(DNS total)	Indicates the number of half-open connections and total number of DNS connections of DNS applications.
Total delay	Indicates delays of all protocols in milliseconds, including the minimum delay, average delay, maximum delay, and delay count.
TCP delay	Indicates TCP delays in milliseconds, including the minimum delay, average delay, maximum delay, and delay count.
UDP delay	Indicates UDP delays in milliseconds, including the minimum delay, average delay, maximum delay, and delay count.

DNS delay	Indicates delays of DNS applications in milliseconds, including the minimum delay, average delay, maximum delay, and delay count.
Route type	Indicates the name of a routing module.
Total(Output/Input)Mbit	Indicates traffic information of all protocols in Mbps, including the uplink traffic and downlink traffic.
TCP(Output/Input)	Indicates TCP traffic information in Mbps, including the uplink traffic and downlink traffic successively.
UDP(Output/Input)	Indicates UDP traffic information in Mbps, including the uplink traffic and downlink traffic successively.
DNS(Output/Input)	Indicates traffic information of DNS applications in Mbps, including the uplink traffic and downlink traffic successively.

#Display information about the database for MLLB network detection.

```
FS#show mllb detect network database from 2016 3 10 10:0:0
Date & Time                       Interface            Type                                              Total
TCP                       UDP                        DNS
2016-03-10   10:00:13                 Gi0/4                         half-connect-flow-count(unknow/all)                   3/14
0/5                       3/9                        0/2
                                                      delay(min/aver/max/count)ms                              0/51/180/11
0/34/150/5                0/66/180/6                 0/25/40/2
                                                      ref_ip-(output/input)Mbit                                       64/176
64/160                    0/8                        0/0

```

Field description:

Field	Description
Date & Time	Indicates the time of network detection.
Interface	Indicates the interface of a detected network.
Type	Indicates data types, including the number of half-open connections, delay, and routing traffic information.
Total	Indicates information about all protocols.
TCP	Indicates TCP information.
UDP	Indicates information of UDP.
DNS	Indicates UDP information.

9.21 show mllb statistics

Use this command to display statistical information of MLLB egress interfaces.

show mllb statistics

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide

Use this command to display statistical information of MLLB egress interfaces.

Configuration Example

#Display statistical information of MLLB egress interfaces.

```
FS# show mllb statistics
Interface                          Packets      Flows
--------------------------    --------    --------
GigabitEthernet 0/1                6750          879
GigabitEthernet 0/2                6580          871
```

Field description:

Field	Description
Interface	Indicates the name of an interface.
Packets	Indicates packet statistics.
Flows	Indicates statistics about new flow.

10 USER-ROUTE Commands

10.1 deny others

Use this command to enable the exit restriction function.

deny others

Use the **no** form of this command to disable the exit restriction function.

no deny others

Use this command to restore the default configuration.

default deny others

Parameter Description

Parameter	Description
N/A	N/A

Defaults The exit restriction function is disabled by default.

Command Mode User configuration mode

14

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 provides the exit restriction function. In scenarios in which no exit device such as ACE is available, use this command if the exit restriction function needs to be enabled on the gateway. For example, this command can be configured for a user in a user group that is authorized to access the internal network but has no permission to access the external network.

Configuration Example #Configure the exit restriction function for the user group named CNII.

```
FS(config)#user-route user-group cnii
FS(config-user-group)# deny others
```

#Disable the exit restriction function of the user group named CNII.

```
FS(config)#user-route user-group cnii
FS(config-user-group)# no deny other
```

Verification Run the **show user-route configure** command to display the configuration information of USER-ROUTE.

N/A

N/A

N/A

10.2 posterior-line interface

Use this command to configure a posterior line for USER-ROUTE.

posterior-line interface *interface-name*

Use the **no** form of this command to delete a posterior line from USER-ROUTE.

no posterior-line interface *interface-name*

Use this command to restore the default configuration.

default posterior-line interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Indicates the name of an interface.

Defaults No posterior line is configured by default.

Command Mode User group configuration mode

14

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.

Configuration Example #Configure a posterior line named GI0/1 for a user group named CNC.

```
FS(config)#user-route user-group cnc
FS(config-user-group)# posterior-line interface GigabitEthernet 0/1
```

Verification Run the **show user-route configure** command to display the configuration information of USER-ROUTE.

10.3 prior-line interface

Use this command to configure a prior line for USER-ROUTE.

prior-line interface *interface-name*

Use the **no** form of this command to delete a prior line from USER-ROUTE.

no prior-line interface *interface-name*

Use this command to restore the default configuration.

default prior-line interface *interface-name*

Parameter Description

Parameter	Description
interface- name	Indicates the name of an interface.

Defaults No prior line is configured by default.

Command Mode User group configuration mode

14

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.

Configuration Example #Configure a prior line named GI0/1 for a user group named CNII.

```
FS(config)#user-route user-group cnii
FS(config-user-group)# prior-line interface GigabitEthernet 0/1
```

Verification Run the **show user-route configure** command to display the configuration information of USER-ROUTE.

10.4 show user-route configure

Use this command to display the configuration information of USER-ROUTE.

show user-route [**user-group** *user-group-name*] **configure**

Parameter Description

Parameter	Description
user-group-name	Indicates the name of a user group.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

14

Usage Guide If no user group is specified, the configuration information of all user groups are displayed by default. If a user group is specified, the configuration information of the user group is displayed.

Configuration Example #Display the configuration information of USER-ROUTE.

```
FS#show user-route configure
>User-route run state: enable
>Total user-group counts: 4
>User-route load-sharing original
>User-route posterior-line load-balance enable
--------------------------------------------------------------------
User-group: cnii
    State: Active
    Prior-line: GigabitEthernet 0/1, GigabitEthernet 0/2
    Posterior-line: GigabitEthernet 0/7, GigabitEthernet 0/8
    Deny others: No
```

```
User-group: cnc
State: Active
   Prior-line: GigabitEthernet 0/3, GigabitEthernet 0/4
   Posterior-line: GigabitEthernet 0/7, GigabitEthernet 0/8
   Deny others: No

User-group: cmii
   State: Inactive
   Prior-line: GigabitEthernet 0/5, GigabitEthernet 0/6
   Posterior-line: GigabitEthernet 0/7, GigabitEthernet 0/8
   Deny others: No

User-group: intranet
   State: Active
   Prior-line:
   Posterior-line:
Deny others: Yes
```

#Display the configuration information of a specified user group of USER-ROUTE.

```
FS#show user-route user-group cnii configure
User-group: cnii
State: Active
Prior-line: GigabitEthernet 0/1, GigabitEthernet 0/2
Posterior-line: GigabitEthernet 0/7, GigabitEthernet 0/8
Deny others: No
```

Field description:

Field	Description
User-group	Indicates the name of a user group.
State	Indicates the status of a user group.
Prior-line	Indicates information about a prior line.
Posterior-line	Indicates information about a posterior line.
Deny others	Indicates the exit restriction function.

10.5 user-route enable

Use this command to enable USER-ROUTE.

user-route enable

Use the **no** form of this command to disable USER-ROUTE.

no user-route enable

Use this command to restore the default configuration.

default user-route enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

USER-ROUTE is disabled by default.

Command Mode

Global configuration mode

14

Usage Guide

If the device needs to support the user route function, USER-ROUTE needs to be enabled.

⚠ USER-ROUTE, based on the common routing mode, determines the target operator resource of the destination IP address accessed by users. Therefore, the route database or relevant static routes need to be configured on the WAN interface so that flows are routed by USER-ROUTE preferentially.

Configuration Example

#Enable USER-ROUTE.

```
FS(config)# user-route enable
```

#Disable USER-ROUTE.

```
FS(config)#no user-route enable
```

Verification

Run the **show user-route configure** command to check whether USER-ROUTE is enabled.

10.6 user-route load-sharing

Use this command to configure the load balancing mode for USER-ROUTE.

user-route load-sharing [**destination** | **original** | **destination-original**]

Use the **no** form of this command to cancel the load balancing mode of USER-ROUTE.

no user-route load-sharing

Use this command to restore the default configuration.

default user-route load-sharing

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The source IP address-based load balancing is adopted by default.

Command Mode

Global configuration mode

14

Usage Guide USER-ROUTE conducts hashing by using the source IP address for load balancing by default. In this way, the traffic of the same user is balanced to the same egress. If load balancing based on the source IP address is unsatisfactory, you can configure the destination IP address-based load balancing or load balancing based on the source IP address + destination IP address.

Configuration Example #Configure destination IP address-based load balancing for USER-ROUTE.

```
FS(config)# user-route load-sharing destination
```

#Cancel source IP address-based load balancing for USER-ROUTE.

```
FS(config)#no user-route load-sharing
```

Verification Run the **show user-route configure** command to display the configuration information of USER-ROUTE.

N/A

N/A

N/A

10.7 user-route posterior-line load-balance

Use this command to enable load balancing for a posterior line of USER-ROUTE.

user-route posterior-line load-balance enable

Use the **no** form of this command to disable load balancing of a posterior line.

no user-route posterior-line load-balance enable

Use this command to restore the default configuration.

default user-route posterior-line load-balance enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The load balancing function is disabled for posterior lines by default.

Command Mode Global configuration mode

14

Usage Guide Load balancing is disabled for posterior lines by default. If there are multiple posterior lines and these posterior lines are from the same operator or the cross-network access is not slow, load balancing can be enabled. Load balancing is a bandwidth-based policy.

Configuration Example

#Configure load balancing for posterior lines.

```
FS(config)#user-route posterior-line load-balance enable
```

#Disable load balancing for posterior lines.

```
FS(config)# no user-route posterior-line load-balance enable
```

Verification

Run the **show user-route configure** command to display the configuration information of USER-ROUTE.

N/A

N/A

N/A

10.8 user-route user-group

Use this command to configure a user group for USER-ROUTE.

user-route user-group *user-group-name*

Use the **no** form of this command to delete the user group of USER-ROUTE.

no user-route user-group *user-group-name*

Use this command to restore the default configuration.

-

Parameter Description

Parameter	Description
user-group-name	Indicates the name of a user group. The value contains a maximum of 30 characters.

Defaults

N/A

Command Mode

Global configuration mode

14

Usage Guide

⚠ The name of the user group needs to be consistent with that on the SAM device. The user group on the SAM device is called "egress control policy".

Configuration Example

#Configure a user group for USER-ROUTE.

```
FS(config)# user-route user-group test
```

#Delete a user group from USER-ROUTE.

```
FS(config)# no user-route user-group test
```

Verification Run the **show user-route configure** command to display the configuration information of USER-ROUTE

Chapter 7 IPv6 Commands

1 IPv6 Commands

1.1 clear ipv6 neighbors

Use this command to clear the dynamic IPv6 neighbors.

clear ipv6 neighbors [**vrf** *vrf-name*] [**oob**] [*interface-id*]

Parameter Description

Parameter	Description
vrf-name	VRF name. All global IPv6 neighbors are cleared without specified VRF name by default.
oob	Clears the dynamic IPv6 neighbors discovered by neighbors on MGMT interface.
interface-id	Interface name. Clear the dynamically learned IPv6 neighbors on the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide This command does not clear all the dynamic neighbors on authentication VLAN.

Note that the static neighbors will not be cleared.

Configuration Examples The following example clears the dynamic IPv6 neighbors.

```
FS# clear ipv6 neighbors
```

The following example clears the dynamic IPv6 neighbors discovered by neighbors on MGMT interface.

```
FS# clear ipv6 neighbors oob
```

The following example clears the dynamically learned IPv6 neighbors on gigabitEthernet 0/1.

```
FS# clear ipv6 neighbors gigabitEthernet 0/1
```

Related Commands

Command	Description
ipv6 neighbor	Configures the neighbor.
show ipv6 neighbors	Displays the neighbor information.

Platform Description N/A

1.2 clear ipv6 path-mtu

Use this command to clear dynamic path MTU. Use the **no** form of this command to clear all dynamic path MTU.

clear ipv6 path-mtu [**vrf** *vrf-name*] [*ipv6-address*]

clear ipv6 path-mtu all

Parameter

Parameter	Description

Description

vrf *vrf-name*	Specifies the VRF name. By default, it indicates global dynamic path MTU.
ipv6-address	Specifies IPv6 address, whether unicast address or multicast address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example clears global dynamic path MTU.

```
FS# clear ipv6 path-mtu
```

The following example clears global and VRF dynamic path MTU.

```
FS# clear ipv6 path-mtu all
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.3 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to restore the default setting.

ipv6 address ipv6-address/prefix-length

ipv6 address *ipv6-prefix/prefix-length* **eui-64**

ipv6 address *prefix-name sub-bits/prefix-length* [**eui-64**]

no ipv6 address

no ipv6 address *ipv6-address/prefix-length*

no ipv6 address *ipv6-prefix/prefix-length* **eui-64**

no ipv6 address *prefix-name sub-bits/prefix-length* [**eui-64**]

Parameter Description

Parameter	Description
iipv6-prefix	IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
ipv6-address	IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
prefix-length	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of S86 is 0 to 64 or 128 to 128.
prefix-name	The general prefix name. Use the specified general prefix to generate the

	interface address.
sub-bits	The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291.
eui-64	The generated IPV6 address consists of the address prefix and the 64 bit interface ID

Defaults

N/A

Command Mode

Interface configuration mode

Usage Guide

When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface.

The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this command to configure the sub-prefix and the host bit.

If no deleted address is specified when using **no ipv6 address**, all the manually configured addresses will be deleted.

no ipv6 address *ipv6-prefix***/***prefix-length* **eui-64** can be used to delete the addresses configured with **ipv6 address** *ipv6-prefix***/***prefix-length* **eui-64**.

Configuration Examples

```
FS(config-if)# ipv6 address 2001:1::1/64
FS(config-if)# no ipv6 address 2001:1::1/64
FS(config-if)# ipv6 address 2002:1::1/64 eui-64
FS(config-if)# no ipv6 address 2002:1::1/64 eui-64
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.4 ipv6 address autoconfig

Use this command to automatically configure an IPv6 stateless address for a network interface. Use the **no** form of this command to restore the default setting.

ipv6 address autoconfig [**default**]

no ipv6 address autoconfig

Parameter Description

Parameter	Description
default	(Optional) If this keyword is configured, a default routing is generated. Note that only one

	layer3 interface on the entire device is allowed to use the **default** keyword

Defaults N/A

Command Mode Interface configuration mode

Usage Guide The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address. If the RA message contains the flag of the "other configurations", the interface will obtain these "other configurations" through the DHCPv6. The "other configurations" usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc.

Configuration Examples The following example enables IPv6 stateless automatic address and generate a default route on GigabitEthernet 0/1.

```
FS(config-if)# ipv6 address autoconfig default
```

The following example deletes IPv6 stateless automatic address on GigabitEthernet 0/1.

```
FS(config-if)# no ipv6 address autoconfig
```

Related Commands

Command	Description
ipv6 address ipv6-*prefix/prefix-length* [**eui-64**]	Configures the IPv6 address for the interface manually.

Platform Description N/A

1.5 ipv6 icmp error-interval

Use this command to set the frequency with which ICMPv6-oversize error packets are sent. Use the **no** form of this command to restore the default setting.

ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]

no ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]

Use this command to set the frequency with which other ICMPv6 error packets are sent. Use the **no** form of this command to restore the default setting.

ipv6 icmp error-interval *milliseconds* [*bucket-size*]

no ipv6 icmp error-interval *milliseconds* [*bucket-size*]

Parameter Description

Parameter	Description
milliseconds	Sets the refresh interval of the token bucket, in the range from 0 to 2147483647 in the unit of seconds. Setting the value to 0 indicates that the frequency with which ICMPv6 error packets are sent is not fixed.
bucket-size	Sets the number of tokens in the token bucket, in the range from 1 to 200.

Defaults

The default *milliseconds* is 100 and *bucket-size* is 10.

Command Mode

Global configuration mode

Usage Guide

The token bucket algorithm is adopted to set the frequency with which ICMPv6 error packets are sent so as to prevent Denial of Service (DoS) attack,

If the forwarded IPv6 packet is greater than the egress IPv6 MTU in size, the router discards the IPv6 packet and sends the ICMPv6-oversize error packet to the source IPv6 address. This kind of ICMPv6 error packet is used for IPv6 path MTU discovery. If there are too many ICMPv6 error packets, the ICMPv6-oversize error packet may not be sent, causing IPv6 path MTU discovery failure. Therefore, it is recommended to set the frequency of ICMPv6-oversize error packet and other ICMPv6 error packet respectively. Note that ICMPv6 redirect packet is not an ICMPv6 error packet and FS sets the frequency of the ICMPv6 redirect packet the same as that of other ICMPv6 error packet.

For the timer is accurate to 10 milliseconds, it is recommended to set the refresh interval of the token bucket to an integer multiple of 10 milliseconds. If the refresh interval is not an integer multiple of 10 milliseconds, it is converted automatically. For example, the frequency of 1 per five milliseconds turns out to be 2 per 10 milliseconds; the frequency of 3 per 15 milliseconds is converted to 2 per 10 milliseconds.

Configuration Examples

The following example sets the frequency with which ICMPv6-oversize error packets are sent to 100 per second.

```
FS(config)# ipv6 icmp error-interval too-big 1000 100
```

The following example sets the frequency with which other ICMPv6 error packets are sent to 10 per second.

```
FS(config)# ipv6 icmp error-interval 1000 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.6 ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the **no** form of this command to restore the default setting.

ipv6 enable

no ipv6 enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface.

> If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with **no ipv6 enable**.

Configuration Examples

```
FS(config-if)# ipv6 enable
```

Related Commands

Command	Description
show ipv6 interface	Displays the related information of an interface.

Platform Description

N/A

1.7 Ipv6 gateway

Use this command to configure the default gateway IPv6 address on the management port.

ipv6 gateway *ipv6-address*

Parameter Description

Parameter	Description
ipv6-address	Configures the default gateway IPv6 address.

Defaults

N/A

Command Mode

Interface configuration mode

Usage Guide

The management port is MGMT in type and 0 in ID.

Configuration Examples

The following example configures the default gateway IPv6 address on the management port.

```
FS(config)# interface mgmt 0
FS(config-int)# ipv6 gateway 2001:1::1
FS(config-int)# exit
FS(config)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.8 ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

no ipv6 general-prefix *prefix-name ipv6-prefix/prefix-length*

Parameter Description

Parameter	Description
prefix-name	The general prefix name.
pv6-prefix	The network prefix value of the general-prefix following the format defined in RFC4291.
prefix-length	The length of the general prefix.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.

A general prefix could contain multiple prefixes.

These longer specified prefixes are usually used for the Ipv6 address configuration on the interface.

Configuration Examples The following example configures manually a general prefix as my-prefix.

```
FS(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

Related Commands

Command	Description
ipv6 address prefix-name sub-bits/prefix-length	Configures the interface address using the general prefix.
show ipv6 general-prefix	Displays the general prefix.

Platform Description N/A

1.9 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.

ipv6 hop-limit *value*

no ipv6 hop-limit

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default is 64.

Command Mode

Global configuration mode.

Usage Guide

This command takes effect for the unicast messages only, not for multicast messages.

Configuration Examples

```
FS(config)# ipv6 hop-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.10 ipv6 mtu

Use this command to configure the MTU of IPv6 packets. Use the **no** form of this command to restore the default setting.

ipv6 mtu *bytes*

no ipv6 mtu

Parameter Description

Parameter	Description
bytes	MTU of IPv6 packets, in bytes. The value ranges from 1280 to 1500.

Defaults

The default configuration is the same as the configuration of the **mtu** command.

Command Mode

Interface configuration mode

Usage Guide

If the size of an IPv6 packet exceeds the IPv6 MTU, the FSOS software segments the packet. For all devices in the same physical network segment, the IPv6 MTU of the interconnected interface must be the same.

Configuration Examples

The following example sets the IPv6 MTU of the FastEthernet 0/1 interface to 1400 bytes.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# ipv6 mtu 1400
```

Related Commands

Command	Description
mtu	Sets the MTU of an interface.

Platform Description

This command cannot be used on Layer 2 devices.

1.11 ipv6 nd cache interface-limit

Use this command to set the maximum number of neighbors learned on the interface. Use the **no** form of this command to restore the default setting.

ipv6 nd cache interface-limit value

no ipv6 nd cache interface-limit

Parameter Description

Parameter	Description
value	Sets the maximum number of neighbors learned on the interface, including the static and dynamic neighbors, in the range from 0 to the number supported by the device. 0 indicates the number is not limited.

Defaults The default is 0.

Command Mode Interface configuration mode

Usage Guide This function can prevent neighbor entries generated by malicious neighbor attacks from consuming memory. The limit number must be no smaller than the number of neighbors learned on the interface. Otherwise, the configuration does not take effect.

Configuration Examples The following example sets the number of neighbors learned on the interface to 100.

```
FS(config)# interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.12 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.

ipv6 nd dad attempts value

no ipv6 nd dad attempts

Parameter Description

Parameter	Description
value	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

Defaults The default is 1.

Command Mode

Interface configuration mode.

Usage Guide

When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the “tentative” status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

Configuration Examples

```
FS(config-if)# ipv6 nd dad attempts 3
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description

N/A

1.13 ipv6 nd dad retry

Use this command to set the interval for address conflict detection. Use the **no** form of this command to restore the default setting.

ipv6 nd dad retry *value*

no ipv6 nd dad retry

Parameter Description

Parameter	Description
value	Sets the interval for address conflict detection, 60 seconds by default. Setting *value* to 0 indicates that the function is disabled.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Before configuring a new IPv6 address for an interface, enable address conflict detection on the interface. If a conflict address is detected, the device does not receive the IPv6 packet destined to the conflict address. This command is used to perform conflict detection again when the interval expires. If there is no conflict, the address can be used.

Configuration Examples

The following example sets the interval for address conflict detection to 10s.

```
FS(config)# ipv6 nd dad retry 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.14 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag bit of the RA message. Use the **no** form of this command to restore the default setting.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Interface configuration mode.

Usage Guide

This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it does not be used.

Configuration Examples

```
FS(config-if)# ipv6 nd managed-config-flag
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.
ipv6 nd other-config-flag	Sets the flag for obtaining all information except IP address through stateful auto configuration.

Platform Description

N/A

1.15 ipv6 nd max-opt

Use this command to configure the max number of ND options to be processed. Use the **no** form of this command to restore the default setting.

ipv6 nd max-opt *value*

no ipv6 nd max-opt

Parameter Description

Parameter	Description
value	Option number, range: 1-100

Defaults

10 options

Command Mode

Global configuration mode.

Usage Guide

This command is used to configure the max number of ND options, for example, source address, MTU, redirection and prefix options.

Configuration Examples

The following example configures the option number to 20.

```
FS(config)# ipv6 nd max-opt 20
```

Related Commands

Command	Description
show run	Displays the configuration status

Platform Description

N/A

1.16 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the **no** form of this command to restore the default setting.

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

Parameter Description

Parameter	Description
milliseconds	Interval for retransmitting NS in the range of 1000 to 429467295 milliseconds

Defaults

The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1000 milliseconds (1 second).

Command mode

Interface configuration mode.

Usage Guide

The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.

Configuration Examples

```
FS(conifig-if)# ipv6 nd ns-interval 2000
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

1.17 ipv6 nd other-config-flag

Use this command to set "other stateful configuration" flag bit of the RA message. Use the **no** form of this command to delete the flag bit.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameter Description

Parameter	Description
N/A	N/A

Defaults The flag bit is not set by default.

Command mode Interface configuration mode.

Usage Guide With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set

Configuration Examples

```
FS(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

1.18 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the **no** form of this command to delete the set prefix or restore the default setting.

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**] | [**pool** *pool-name*]]

no ipv6 nd prefix { *ipv6-prefix/prefix-length* | **default** }

Parameter Description

Parameter	Description
ipv6-prefix	IPv6 network ID following the format defined in RFC4291
prefix-length	Length of the IPv6 prefix. "/" shall be added in front of the prefix

valid-lifetime	Valid lifetime of the RA prefix received by the host
preferred-lifetime	Preferred lifetime of the RA prefix received by the host
at *valid-date preferred-date*	Sets the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
infinite	Indicates that the prefix is always valid.
default	Sets the default prefix.
no-advertise	The prefix will not be advertised by the device.
off-link	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
no-autoconfig	Indicates that the RA prefix received by the host cannot be used for auto address configuration.
pool pool-name	Indicates the IPv6 prefix pool

Defaults

By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:
valid-lifetime: 2592000s (30 days)
preferred-lifetime: 604800s (7 days),
The prefix is advertised and is used for on-link judgment and auto address configuration.

Command Mode

Interface configuration mode.

Usage Guide

This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

ipv6 nd prefix default

Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

at *valid-date preferred-date*

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

Configuration Examples

The following example adds a prefix for SVI 1.

```
FS(config)# interface vlan 1
FS(conifig-if)# ipv6 nd prefix 2001::/64 infinite 2592000
```

The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration):

```
FS(config)# interface vlan 1

FS(config-if)# ipv6 prefix default no-autoconfig
```

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

Related Commands

Command	Description
show ipv6 interface	Displays the RA information of an interface.

Platform Description

N/A

1.19 ipv6 nd ra-hoplimit

Use this command to set the hopcount of the RA message. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-hoplimit *value*

no ipv6 nd ra-hoplimit

Parameter Description

Parameter	Description
value	Hopcount

Defaults

The default is 64.

Command Mode

Interface configuration mode.

Usage Guide

This command is used to set the hopcount of the RA message.

Configuration Examples

```
FS(config -if)# ipv6 nd ra-hoplimit 110
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.
ipv6 nd ra-lifetime	Sets the lifetime of the device.
ipv6 nd ra-interval	Sets the interval of sending the RA message.
ipv6 nd ra-mtu	Sets the MTU of the RA message.

Platform Description

N/A

1.20 ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-interval { *seconds* | **min-max** *min_value max_value* }

no ipv6 nd ra-interva l

Parameter Description

Parameter	Description
seconds	Interval of sending the RA message in seconds, 3-1800s.
min-max	Maximum and minimum interval sending the RA message in seconds
min_value	Minimum interval sending the RA message in seconds
max_value	Maximum interval sending the RA message in seconds

Defaults

200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.

Command Mode

Interface configuration mode.

Usage Guide

If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value.

If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

Configuration Examples

```
FS(conifig-if)# ipv6 nd ra-interval 110
FS(config-if)# ipv6 nd ra-interval min-max 110 120
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.
ipv6 nd ra-lifetime	Sets the lifetime of the device.
ipv6 nd ra-hoplimit	Sets the hopfcount of the RA message.
ipv6 nd ra-mtu	Sets the MTU of the RA message.

Platform Description

N/A

1.21 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime

Parameter Description

Parameter	Description
seconds	Default life time of the device on the interface, in the range from 0 to 9000 in the unit of seconds.

Defaults The default is 1800.

Command Mode Interface configuration mode.

Usage Guide The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)

Configuration Examples

```
FS(conifig-if)# ipv6 nd ra-lifetime 2000
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.
ipv6 nd ra-interval	Sets the interval of sending the RA.
ipv6 nd ra-hoplimit	Sets the hopcount of the RA.
ipv6 nd ra-mtu	Sets the MTU of the RA.

Platform Description N/A

1.22 ipv6 nd ra-mtu

Use this command to set the MTU of the RA message. Use the **no** form of this command to restore the default setting.

ipv6 nd ra-mtu *value*

no ipv6 nd ra-mtu

Parameter Description

Parameter	Description
value	MTU value, in the range from 0 to 4294967295.

Defaults IPv6 MTU value of the network interface.

Command Mode Interface configuration mode.

Usage Guide If it is specified as 0, the RA will not have the MTU option

Configuration Examples

```
FS(config -if)# ipv6 nd ra-mtu 1400
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.
ipv6 nd ra-lifetime	Sets the lifetime of the device.
ipv6 nd ra-interval	Sets the interval of sending the RA message.
ipv6 nd ra-hoplimit	Sets the hopcount of the RA message.

Platform Description

N/A

1.23 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the **no** form of this command to restore the default setting.

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

Parameter Description

Parameter	Description
milliseconds	Reachable time for the neighbor in the range from 0 to 3600000 in the unit of milliseconds.

Defaults

The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30000 milliseconds (30 seconds) when the device discovers the neighbor.

Command Mode

Interface configuration mode.

Usage Guide

The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time.

The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used.

According to RFC 4861, the actual time to reach neighbor is not consistent with the configured value, ranging from 0.5*configured value to 1.5*configured value.

Configuration Examples

```
FS(config-if)# ipv6 nd reachable-time 1000000
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform

N/A

Description

1.24 ipv6 nd stale-time

Use this command to set the period for the neighbor to maintain the state. Use the **no** form of this command to restore the default setting.

ipv6 nd stale-time *seconds*

no ipv6 nd stale-time

Parameter Description

Parameter	Description
Seconds	Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds.

Defaults The default is 3600.

Command Mode Global configuration mode, interface configuration mode

Usage Guide This command is used to set the period for the neighbor to maintain the state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small.

Configuration Examples The following example globally sets the period to 600 seconds for the neighbor to maintain the state.

```
FS(config)# ipv6 nd stale-time 600
```

The following example sets on VLAN 1 the period to 600 seconds for the neighbor to maintain the state.

```
FS(config-if-VLAN 1)# ipv6 nd stale-time 600
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.25 ipv6 nd suppress-auth-vlan-ns

Use this command to disable the SVI interface from sending the NS packet to the authentication VLAN. Use the **no** form of this command to disable this function.

ipv6 nd suppress-auth-vlan-ns

no ipv6 nd suppress-auth-vlan-ns

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide This command is supported on the SVI interface in gateway authentication mode.

Configuration Examples The following example enables VLAN 2 to send the NS packet to the authentication VLAN.

```
FS(config-if-VLAN 2)# no ipv6 nd suppress-auth-vlan-ns
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.26 ipv6 nd suppress-ra

Use this command to disable the interface from sending the RA message. Use the **no** form of this command to enable the function.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameter Description

Parameter	Description
N/A	N/A

Defaults The **ipv6 nd suppress-ra** command is enabled by default.

Command Mode Interface configuration mode.

Usage Guide This command suppresses the sending of the RA message on an interface.

Configuration Examples

```
FS(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

1.27 ipv6 nd threshold

Use this command to configure the neighbor entry threshold to prevent ND-based Dos attacks. Use the **no** form of this command to restore the default setting.

ipv6 nd threshold *percent_value*

no ipv6 nd threshold

Parameter Description

Parameter	Description
percent_value	Neighbor entry threshold, in the range from 50 to 100.

Defaults

The default is 70.

Command Mode

Global configuration mode.

Usage Guide

The threshold indicates the percentage of current neighbor entry count accounting for the maximum count. When the IPv6 neighbor entry count reaches the threshold, reachability test will be performed on neighbors in the stale state. But it does not affect the neighbor discovery function. The device can still learn new neighbor entries.

Configuration Examples

The following example sets the threshold to 80%.

```
FS(config)# ipv6 nd threshold 80
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.28 ipv6 nd threshold per-mac

Use this command to configure the maximum neighbor entry count for a MAC address to prevent ND-based Dos attacks. Use the **no** form of this command to restore the default setting.

ipv6 nd threshold per-mac *value*

no ipv6 nd threshold per-mac

Parameter Description

Parameter	Description
value	Neighbor entry count, in the range from 4 to 256.

Defaults

The default is 16.

Command Mode

Global configuration mode.

Usage Guide

When the IPv6 neighbor entry count reaches the threshold, reachability test will be performed on neighbors in the stale state. But it does not affect the neighbor discovery function. The device can still learn new neighbor entries.

Configuration Examples

The following example sets the count to 100.

```
FS(config)# ipv6 nd threshold per-mac 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.29 ipv6 nd unresolved

Use this command to set the maximum number of the unresolved neighbor table entries. Use the **no** form of this command to restore the default setting.

ipv6 nd unresolved *number*

no ipv6 nd unresolved

Parameter Description

Parameter	Description
number	Sets the maximum number of the unresolved neighbor table entries, in the range from 1 to the neighbor table size supported by the device.

Defaults

The default is 0. (The maximum number is the neighbor table size supported by the device)

Command Mode

Global configuration mode

Usage Guide

This command is used to prevent unresolved ND table entries generated by malicious scan attacks from consuming table entry resources.

Configuration Examples

The following example sets the maximum number of the unresolved neighbor table entries to 200.

```
FS(config)# ipv6 nd unresolved 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.30 ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to delete a static neighbor.

ipv6 neighbor *ipv6-address interface-id hardware-address*

no ipv6 neighbor *ipv6-address interface-id*

Parameter Description

Parameter	Description
ipv6-address	The neighbor IPv6 address, in the form as defined in RFC 4291.
interface-id	Specifies the network interface where the neighbor is (including Router Port, L3 AP port and SVI interface).
hardware-address	The 48-bit MAC address, a dotted triple of four-digit hexadecimal numbers.

Defaults

No static neighbor is configured by default.

Command Mode

Global configuration mode

Usage Guide

This command can only be configured on the interface enabled with IPv6 protocol, similar to the ARP command.

If the neighbor to be configured has been learned through Neighbor Discovery Protocol (NDP) and stored in the NDP neighbor table, the dynamic neighbor turns to be static. If the static neighbor is valid, it is always reachable. An invalid static neighbor refers to the neighbor whose IPv6 address is not valid (not in the IPv6 network segment configured for the interface or interface address conflict). The packet is not forwarded to the MAC address as specified by the invalid static neighbor. The invalid static neighbor is in inactive state. Use the show ipv6 neighbor static command to display the state of the static neighbor.

Use the **clear ipv6 neighbors** command to clear all neighbors learned dynamically through NDP.

Configuration Examples

The following example configures a static neighbor on SVI 1.

```
FS(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.31 ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests. Use the **no** form of this command to use the global IP address w as the source address to send neighbor requests.

ipv6 ns-linklocal-src

no ipv6 ns-linklocal-src

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The local address of the link is always used as the source address to send neighbor requests.

Command

Global configuration mode.

Mode

Usage Guide N/A

Configuration Examples

```
FS(config)# ipv6 ns-linklocal-src
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.32 ipv6 path-mtu

Use this command to configure static path MTU. Use the **no** form of this command to remove the setting.

ipv6 path-mtu [**vrf** *vrf-name*] *ipv6-address value*

no ipv6 path-mtu [**vrf** *vrf-name*] *ipv6-address*

Use this command to clear all static path MTUs.

no ipv6 path-mtu all

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies VRF name, By default, it indicates global path MTU.
ipv6-address	Specifies IPv6 address, whether unicast address or multicast address.
value	Sets the MTU value in the unit of bytes, in the range from 1280 to 65575.

Defaults N/A

Command Mode Global configuration mode

Usage Guide When the source host sends a packet from an interface, it compares the IPv6 MTU of the interface with the path MTU. If the packet is longer than the smaller MTU, the smaller MTU is adopted to perform fragmentation.

The IPv6 multicast packets may reach different nodes through different paths, Therefore, the path MTU of the multicast address should be the smallest among all path MTUs.

If VRF name and IPv6 address are both the same, the static path MTU overwrites the dynamic path MTU,

You can use the **no ipv6 path-mtu all** command to delete all static path MTU.

You can use the **show ipv6 path-mtu statistics** command to display the maximum number and current number of static path MTU.

Configuration Examples The following example sets the path MTU for IPv6 A000::1 to 1400 bytes.

```
FS(config)# ipv6 path-mtu A000::1 1400
```

Related

Command	Description

Commands

N/A	N/A

Platform Description

N/A

1.33 ipv6 path-mtu age

Use this command to configure the aging time for dynamic path MTU. Use the **no** or **default** form of this command to restore the default setting.

ipv6 path-mtu age { *age-time* | **infinity** }

no ipv6 path-mtu age

default ipv6 path-mtu age

Parameter Description

Parameter	Description
age-time	Sets the aging time for dynamic path MTU, in the range from 10 to (30 * 24 * 60) in the unit of minutes.
infinity	Indicates no aging.

Defaults

The default is 10 minutes,

Command Mode

Global configuration mode

Usage Guide

Before the aging time expires, the path MTU decreases.

In the actual application, the network topology and route may change, causing path change. The MTU of the learnt path may be smaller than the actual path MTU. Therefore, the path MTU should be aged out periodically and learnt again.

When the aging time expires, the corresponding path MTU is cleared. Before learning a new path MTU, the long IPv6 packet may be discarded by the router during forwarding. If the LAN is connected to the Internet through a link with a small MTU, which is the smallest among all path MTUs, you should increase the aging time or even set it to **infinity**.

Configuration Examples

The following example sets the aging time of dynamic path MTU to 20 minutes.

```
FS(config)#ipv6 path-mtu age 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.34 ipv6 redirects

Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the **no** form of this command to restore the default setting.

ipv6 redirects

no ipv6 redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide The transmission rate of any ICMPv6 error message is limited. By default, it is 10pps.

Configuration Examples The following example enables ICMPv6 redirection on interface GigabitEthernet 0/1.

```
FS(config-if-GigabitEthernet 0/1)# ipv6 redirects
```

Related Commands

Command	Description
show ipv6 interface	Displays the interface information.

Platform Description N/A

1.35 ipv6 source-route

Use this command to forward the IPv6 packet with route header. Use the **no** form of this command to restore the default setting.

ipv6 source-route

no ipv6 source-route

Parameter Description

Parameter	Description
N/A	N/A

Defaults The **ipv6 source-route** command is disabled by default.

Command Mode Global configuration mode.

Usage Guide Because of the potential security of the header of type 0 route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.

Configuration Examples

```
FS(config)# no ipv6 source-route
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.36 ipv6 unnumbered

Use this command to enable the interface to use the address of a specified interface as the source address. Use the **no** form of this command to restore the default setting.

ipv6 unnumbered *interface-id*

no ipv6 unnumbered

Parameter Description

Parameter	Description
interface-id	Specifies the interface (including the Ethernet interface, aggregate port and SVI interface).

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode.

Usage Guide

This command is used to save IPv6 addresses and only supported on PPP interfaces.

Configuration Examples

The following example enables Virtual-Template 1 to use the IP address of loopback 1 as the source address.

```
FS(config-if-Virtual-Template 1)#ipv6 unnumbered loopback 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on only routers.

1.37 peer default ipv6 pool

Use this command to enable the device to obtain a prefix from the prefix pool when sending RA packets. Use the **no** form of this command to restore the default setting.

peer default ipv6 pool *pool-name*

no peer default ipv6 pool

Parameter Description

Parameter	Description
pool-name	Specifies the prefix pool name, which is configured by using the **ipv6 local pool** command.

Defaults

This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide This command is applied in the IPv6 over VPDN scenario.

Configuration Examples The following example enables Virtual-Template 1 to obtain a prefix from prefix pool **rapool** when sending RA packets.

```
FS(config-if-Virtual-Template 1)# peer default ipv6 pool rapool
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on only routers.

1.38 show ipv6 address

Use this command to display the IPv6 addresses.

show ipv6 address [*interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays all IPv6 address configured on the device.

```
FS#show ipv6 addr
Global unicast address limit: 1024, Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
  GigabitEthernet 0/5
    2003:1::23/64                                Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
    fe80::2d0:f8ff:fefb:deb2/64                  Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

```
    2005:1::1111/64                              Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
FS#
```

The following example displays the IPv6 address configured on the GigabitEthernet 0/1.

```
FS#show ipv6 addr gi 0/5
Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
    2003:1::23/64                                Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
    fe80::2d0:f8ff:fefb:deb2/64                  Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
    2005:1::1111/64                              Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
FS#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.39 show ipv6 general-prefix

Use this command to display the information of the general prefix.

show ipv6 general-prefix

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the information of the general prefix including the manually configured and learned from the DHCPv6 agent.

Configuration Examples

```
The following example displays the information of the general prefix.FS# show ipv6 general-prefix
There is 1 general prefix.
```

```
IPv6 general prefix my-prefix, acquired via Manual configuration
 2001:1111:2222::/48
 2001:1111:3333::/48
```

Related Commands

Command	Description
ipv6 general-prefix	Configures the general prefix.

Platform Description

N/A

1.40 show ipv6 interface

Use this command to display the IPv6 interface information.

show ipv6 interface [*interface-id*] [**ra-info**]] [*brief* [interface-id]]

Parameter Description

Parameter	Description
interface-id	Interface (including Ethernet interface, aggregate port, or SVI)
ra-info	Displays the RA information of the interface.
brief	Displays the brief information of the interface (interface status and address information).

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to display the address configuration, ND configuration and other information of an IPv6 interface.

Configuration Examples

The following example displays the information of the IPv6 interface.

```
FS# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
```

```
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 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<240--160>
ND device advertisements live for 1800 seconds
```

The following line is included in the above information: 2001::1, subnet is 2001::/64 [**TENTATIVE**]. The flag bit in the [ ] following the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	Indicate that the address is an anycast address.
TENTATIVE	Indicate that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	Indicate that a duplicate address exists.
DEPRECATED	Indicate that the preferred lifetime of the address expires.
NODAD	Indicate that no DAD is implemented for the address.
AUTOIFID	Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.

The following example displays the RA information of the IPv6 interface.

```
FS# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
ND device advertisements are sent every 200 seconds<240--160>
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)
fec0:1:1:1::/64(Def,Auto,vltime: 2592000, pltime: 604800, flags: LA)
```

Description of the fields in **ra-info**:

Field	Meaning

RA timer is stopped (on)	Indicate whether the RA timer is started.
waits	Indicate that the RS is received but the number of the responses is not available.
initcount	Indicate the number of the RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: Indicate the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M | M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O | O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

Field	**Meaning**
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	Indicate that the interfaces use the default prefix.
Auto | CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
!Adv	Indicate that the prefix will not be advertised.
vltime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.
L | !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
A | !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

The following example displays the brief information of the IPv6 interface.

```
FS#show ipv6 interface brief

GigabitEthernet 0/1              [down/down]
        2222::2
        FE80::1614:4BFF:FE5C:ED3A
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.41 show ipv6 neighbors

Use this command to display the IPv6 neighbors.

show ipv6 neighbors [**vrf** *vrf-name*] [**verbose**] [*interface-id*] [*ipv6-address*] [**static**] [**oob**]

Parameter Description

Parameter	Description
verbose	Displays the neighbor details.
static	Displays the validity status of static neighbors.
vrf-name	VRF name
interface-id	Displays the neighbors of the specified interface.
ipv6-addres	Displays the neighbors of the specified IPv6 address.
static	Displays the effectiveness of static neighbors.
oob	Displays the IPv6 neighbors of MGMTport.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following example displays the neighbors on the SVI 1 interface:FS# show ipv6 neighbors vlan 1

```
IPv6 Address Linklayer Addr Interface
fa::1 00d0.0000.0002 vlan 1
fe80::200:ff:fe00:2 00d0.0000.0002 vlan 1
```

Show the neighbor details:

```
FS# show ipv6 neighbors verbose
IPv6 Address Linklayer Addr Interface
2001::1 00d0.f800.0001 vlan 1
  State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1 00d0.f800.0001 vlan 1
  State: Reach/H Age: - asked: 0
```

Field	Meaning
IPv6 Address	IPv6 address of the Neighbor
Linklayer Addr	Link address, namely, MAC address. If it is not available, incomplete is displayed.

Interface	Interface the neighbor locates.
State	State of the neighbor: state/H(R) The values of STATE are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3). ?: Unknown state. /R—indicate the neighbor is considered as a device /H: The neighbor is a host.
Age	The reachable time of the neighbor. ’-‘ indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. ’expired’ indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.
Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

Related Commands

Command	Description
ipv6 neighbor	Configures a neighbor.

Platform Description

N/A

1.42 show ipv6 neighbors statistics

Use the following commands to display the statistics of IPv6 neighbors.

show ipv6 neighbors [**vrf** *vrf-name*] **statistics** [**all**]

Parameter Description

Parameter	Description
vrf-name	VRF name
all	Displays the statistics of all IPv6 neighbors.

Defaults

N/A

Command

Privileged EXEC mode.

Mode

Usage Guide N/A

Configuration Examples

The following example displays the statistics of the global neighbors.

```
FS#show ipv6 neighbor statistics

Memory: 0 bytes
Entries: 0
   Static: 0,Dynamic: 0,Local: 0
   Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0
FS#
```

The following example displays the statistics of all IPv6 neighbors.

```
FS#show ipv6 neighbor statistics all

IPv6 neighbor table count: 1
Static neighbor count: 0(0 active, 0 inactive)
Total
Memory: 0 bytes
Entries: 0
   Static: 0,Dynamic: 0,Local: 0
   Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;

Global
Memory: 0 bytes
Entries: 0
   Static: 0,Dynamic: 0,Local: 0
   Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
FS#
```

Related Commands

Command	Description
N/A	N/A

Platform Description Supported on all platforms.

1.43 show ipv6 packet statistics per-mac

Use this command to display the number of neighbor entries of every MAC address.

show ipv6 neighbor statistics per-mac [*interface-name*] [*mac-address*]

Parameter Description

Parameter	Description
interface-name	Interface ID

mac-address	MAC address

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the number of neighbor entries of every MAC address..

```
FS# show ipv6 neighbor statistics per-mac
Interface    MAC address          Statistics
------------------------------------------------
VLAN 1    0000:0000:0001      3
VLAN 1    0000:0000:0002      5
VLAN 2    0000:0000:0003      10
```

Field	Description
Interface	Interface ID.
MAC address	MAC address.
Statistics	ND entry number.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.44 show ipv6 packet statistics

Use this command to display the statistics of IPv6 packets.

show ipv6 packet statistics [**total** | *interface-name*]

Parameter Description

Parameter	Description
total	Displays total statistics of all interfaces.
interface-name	Interface name

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

The following example displays the total statistics of the IPv6 packets and the statistics of each inerface.

```
 FS#show ipv6 pack statistics
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
  GigabitEthernet 0/5
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
FS#
```

The following example displays the total statistics of the IPv6 packets.

```
FS#show ipv6 pack statistics total
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
FS#
```

Related Commands

Command	Description
N/A	N/A

Platform Description Supported on all platforms.

1.45 show ipv6 path-mtu

Use this command to display path MTU information.

show ipv6 path-mtu [**vrf** *vrf-name*] [*ipv6-address* | **dynamic** | **static**]

Parameter Description

Parameter	Description
vrf *vrf-name*	Specifies the VRF name. By default, global path MTU information is displayed.
ipv6-address	Specifies the IPv6 address.
dynamic	Displays dynamic path MTU.
static	Displays static path MTU.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays global path MTU information.

```
FS#show ipv6 path-mtu
IPv6 Address     MTU     Age     Type
A000::1          1400    --      Static
A000::2          1300    1       Dynamic
```

Field	Description
IPv6 Address	IPv6 address
MTU	Path MTU
Age	Aging time, the time interval from learning the dynamic path MTU until now in the unit of minutes, If it is a static path MTU, "--" is displayed.
Type	Path MTU type: dynamic or static.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.46 show ipv6 path-mtu statistics

Use this command to display path MTU statistics.

show ipv6 path-mtu statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays path MTU statistics.

```
FS#show ipv6 path-mtu statistics
Maximum count: static 8192, dynamic 8192
VRF         Static     Dynamic      Sum
--------------------------------
Global     10           20               30
AAA         20           30               50
--------------------------------
Total       30           50               80
```

Field	Description
Maximum count: static 8192, dynamic 8192	The maximum numbers of dynamic and static path MTU are 8192 respectively.
VRF	VRF name.
Static	The number of static path MTU.
Dynamic	The number of dynamic path MTU.
Sum	The number of dynamic and static path MTU.
Total	The number of global and VRF path MTU.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.47 show ipv6 raw-socket

Use this command to display all IPv6 raw sockets.

show ipv6 raw-socket [*num*]

Parameter Description

Parameter	Description
num	Protocol.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays all IPv6 raw sockets.

```
FS# show ipv6 raw-socket
Number Protocol Process name
1         ICMPv6     vrrp.elf
2         ICMPv6     tcpip.elf
3         VRRP       vrrp.elf
Total: 3
```

Field	Description
Number	Number.
Protocol	Protocol.
Process name	Process number.
Total	Total number of IPv6 raw sockets.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.48 show ipv6 routers

In the IPv6 network, some neighbor routers send out the advertisement messages. Use this command to display the neighbor routers and the advertisement.

show ipv6 routers [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	(Optional) Displays the routing advertisement of the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to display the neighbor routers and the routing advertisement. If no interface is specified, all the routing advertisement of this device will be displayed.

Configuration Examples

The following example displays the IPv6 router

```
FS# show ipv6 routers
Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec
  Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500
  Preference=MEDIUM
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 6001:3::/64 onlink autoconfig
  Valid lifetime 2592000 sec, preferred lifetime 604800 sec
  Prefix 6001:2::/64 onlink autoconfig
Valid lifetime 2592000 seconds, preferred lifetime 604800 seconds
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.49 show ipv6 sockets

Use this command to display all IPv6 sockets.

show ipv6 sockets

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following example displays all IPv6 sockets.

```
FS# show ipv6 sockets
Number Process name     Type    Protocol  LocalIP:Port  ForeignIP:Port  State
1      vrrp.elf         RAW     ICMPv6    :::58         :::0            *
2      tcpip.elf        RAW     ICMPv6    :::58         :::0            *
3      vrrp.elf         RAW     VRRP      :::112        :::0            *
4      fs-snmpd         DGRAM   UDP       :::161        :::0            *
5      rg-snmpd         DGRAM   UDP       :::162        :::0            *
6      dhcp6.elf        DGRAM   UDP       :::547        :::0            *
7      fs-sshd          STREAM  TCP       :::22         :::0            LISTEN
8      fs-telnetd       STREAM  TCP       :::23         :::0            LISTEN
Total: 8
```

Field	Description
Number	Number.
Process name	Process name.
Type	Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type.
Protocol	Protocol number
LocalIP:Port	Local IPv6 address and port.
ForeignIP:Port	Peer IPv6 address and port.
State	State (for IPv6 TCP sockets).
Total	Total number of sockets.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.50 show ipv6 udp

Use this command to display all IPv6 UDP sockets.

show ipv6 udp [**local-port** *num*] [**peer-port** *num*]

Use this command to display IPv6 UDP socket statistics.

show ipv6 udp statistics

Parameter Description

Parameter	Description
local-port *num*	Local port number.
peer-port *num*	Peer port number.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays all IPv6 UDP sockets.

```
FS# show ipv6 udp
Number Local Address     Peer Address     Process name
1          :::161              :::0            fs-snmpd
2          :::162              :::0            fs-snmpd
3          :::547              :::0            dhcp6.elf
```

Filed	Description
Number	Number.
Local Address	Local IPv6 address and port.
Peer Address	Peer IPv6 address and port.
Process name	Process name.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

Chapter 8 Network Management Commands

1 RLOG Commands

1.1 ip nat-log on

Use this command to record only NAT logs.

Use the **no** form of this command to disable the recording of only NAT logs.

ip nat-log on

no ip nat-log on

Parameter Description

Parameter	Description
N/A	N/A

Defaults The recording of only NAT logs is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Configure this function to record only NAT logs. After this function is disabled, all flow logs are recorded.

Configuration Examples The following example enables the recording of only NAT logs.

```
FS(config)# ip nat-log on
```

Verification Run the **show nat-log status** command to check whether the recording of only NAT logs is enabled.

1.2 nat-log data-store

Use this command to set the NAT log storage period in days.

Use the **no** form of this command to restore the default configuration.

nat-log data-store *days*

no nat-log data-store

Parameter Description

Parameter	Description
days	Log storage period in days. The value ranges from **10** to **90**.

Defaults The NAT logs are stored for 30 days by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The NAT log storage period can be properly adjusted according to the disk capacity and query requirement.

Configuration Examples

The following example sets the NAT log storage period to 60 days.

```
FS(config)# nat-log data-store 60
```

Verification

Run the **show run** command to check the currently configured NAT log storage period.

1.3 nat-log enable

Use this command to enable NAT logging.

Use the **no** form of this command to disable NAT logging.

nat-log enable

no nat-log enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

NAT logging is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Run this command to record NAT logs locally.

Configuration Examples

The following example enables NAT logging.

```
FS(config)# nat-log enable
```

Verification

Run the **show nat-log status** command to check whether NAT logging is enabled.

1.4 rlog dev-ip

Use this command to set the local IP address of the RLOG device.

Use the **no** form of this command to cancel the local IP address of the RLOG device.

rlog dev-ip *ip*

no rlog dev-ip

Parameter Description

Parameter	Description
ip	Local IP address of the RLOG device

Defaults

N/A

Command Mode

Global configuration mode

Default Level 14

Usage Guide The local IP address field is required in some logs. Set this field according to the actual local IP address of the RLOG device.

⚠ The local IP address field is mainly used by the RLOG server. Absence of the field value may cause an information parsing error of the RLOG server.

Configuration Examples The following example sets the local IP address to 10.10.10.2.

```
FS(config)# rlog dev-ip 10.10.10.2
```

Verification Run the **show rlog** command to display the local IP address of the RLOG device.

1.5 rlog export-rate

Use this command to configure the RLOG export rate.

Use the **no** form of this command to cancel the RLOG export rate.

rlog export-rate *val*

no rlog export-rate

Parameter Description

Parameter	Description
val	Number of logs sent per second. The value ranges from **10** to **100,000**.

Defaults The default RLOG export rage is **1000** by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The RLOG export rate is determined according to device performance and log outputs.

⚠ An excessively low rate causes log losses, while an excessively high rate continuously raises CPU usage.

Configuration Examples The following example sets the RLOG export rate to **10,000**.

```
rlog export-rate 10000
```

Verification Run the **show rlog** command to check the current RLOG export rate.

1.6 rlog filter

Use this command to set the condition for filtering flow logs and NAT logs.

Use the **no** form of this command to cancel the condition for filtering flow logs and NAT logs.

rlog filter *aclid*

no rlog filter

Parameter Description

Parameter	Description
aclid	ID of the ACL for filtering. The value ranges from **2000** to **2699.**

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide This function is effective to both flow logs and NAT logs. It is configured when there are excessive flow logs or when not all flow logs need to be recorded.

⚠ The corresponding ACL needs to be preset.

Configuration Examples The following example filters flow logs according to ACL 2000.

```
FS(config)# access-list 2000 permit udp any any
FS(config)# rlog filter 2000
```

Verification Run the **show run** command to check whether the filtering condition is configured.

Common Errors The corresponding ACL is not configured.

The ACL ID is beyond the value range.

1.7 rlog server

Use this command to configure the RLOG server.

Use the **no** form of this command to disable the RLOG server.

rlog server *ip-address* [**oob**] [**port** *port-num*]

no rlog server *ip-address*

Parameter Description

Parameter	Description
Ip-address	IP address of the RLOG server
port-num	Port ID of the RLOG server
oob	OOB interface

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide

To send logs to the RLOG server, configure the IP address, port ID, and other information of the server first.

Configuration Examples

The following example sets the IP address of the RLOG server to 10.10.10.10 and the port ID to 20000.

```
FS(config)# rlog server 10.10.10.10 port 20000
```

Verification

Run the **show rlog** command to check whether the configured server takes effect.

1.8 rlog set

Use this command to configure RLOG combination.

Use the **no** form of this command to disable RLOG combination.

rlog set log-com

no rlog set log-com

Parameter Description

Parameter	Description
N/A	*N/A*

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command needs to be supported by the RLOG server, and can improve the RLOG export efficient cy to some extent.

⚠ If the RLOG server does not support RLOG combination, logs may be lost or fail to be parsed.

Configuration Examples

N/A

Verification

Run the **show rlog** command to check whether RLOG combination is enabled.

1.9 rlog sn-mac-on

Use this command to configure the function of carrying the SN and MAC address in flow logs.

Use the **no** form of this command to cancel the function of carrying the SN and MAC address in flow logs.

rlog sn-mac-on

no rlog sn-mac-on

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The function of carrying the SN and MAC address in flow logs is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide When this function is enabled, flow logs exported to the RLOG server carry the SN and MAC address, so that the RLOG server can parse the flow logs.

Confirm in advance that the RLOG server is compatible with this configuration.

Configuration Examples The following example enables the function of carrying the SN and MAC address in flow logs.

```
FS(config)# rlog sn-mac-on
```

Verification Run the **show run** command to check whether the function of carrying the SN and MAC address in flow logs is configured.

1.10 rlog type

Use this command to configure the RLOG type for RLOG export or file generation.

Use the **no** form of this command to cancel the RLOG type.

rlog type *n* **server** *server-ip* **priority** *prio*

rlog type *n* **file**

no rlog type *n* **server** *server-ip*

no rlog type *n* **file**

Parameter Description

Parameter	Description
n	RLOG type
server-ip	IP address of the configured RLOG server
prio	RLOG export priority. The value ranges from **0** to **7**. A smaller value indicates a higher priority.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is mandatory for RLOG export. Coordination from the RLOG-FILE module is required to export RLOG files.

Configuration Examples The following example configures flow log export to the server at 10.10.10.10.

```
FS(config)# rlog type 16 server 10.10.10.10 priority 1
```

Verification Run the **show rlog-status** command to display RLOG types supported by the RLOG server.

Prompts If the configured RLOG server does not exist, an error prompt is displayed and the configuration does not take effect.

1.11 rlog-file local-path

Use this command to configure the local path for storing RLOG files.

Use the **no** form of this command to cancel the local path for storing RLOG files.

rlog-file local-path *path-string*

no rlog-file local-path

Parameter Description

Parameter	Description
path-string	Local path for storing RLOG files.

Defaults The default local path is **/tmp/rlog-file** in real-time mode and is **/mnt/sata0/rlog-file** in scheduled mode.

Command Mode Global configuration mode

Default Level 14

Usage Guide The real-time mode and scheduled mode have different RLOG file storage requirements. The scheduled mode requires larger storage space, and therefore, RLOG files should be stored in hard disks in this mode.

⚠ If RLOG files are stored in the **tmp** directory in scheduled mode, memory resources may be exhausted, causing a system error.

Configuration Examples The following example configures a hard disk path as the local path for storing RLOG files.

```
FS(config)# rlog-file local-path /mnt/sata0/rlog-file
```

Verification Run the **show rlog-file** command to display the configured local path for storing RLOG files.

1.12 rlog-file send

Use this command to configure the RLOG file export parameters.

Use the **no** form of this command to cancel the configuration of the RLOG file export parameters.

rlog-file send time-range from *from-hour* **to** *to-hour*

rlog-file send compress { zip | none }

rlog-file send format {elog | macc }

no rlog-file send time-range

no rlog-file send compress

no rlog-file send format

Parameter Description

Parameter	Description
from-hour	Start time in the 24-hour system for scheduled RLOG file export

to-hour	End time in the 24-hour system for scheduled RLOG file export. This parameter can be set to a value less than that of **from-hour**, indicating that the export lasts to the next day.

Defaults

By default, the RLOG files are exported in **key-val** format in real-time mode by using FTP and zip compression.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

RLOG file export parameters need to be configured for RLOG export in file mode.

⚠ The parameter values must be agreed on with the RLOG server. Otherwise, RLOG export may fail.

Configuration Examples

1. The following example configures RLOG file export from 22:00 to 06:00 the next day.

```
FS(config)# rlog-file send time-range from 22 to 6
```

2. The following example configures the zip compression mode for RLOG file export.

```
FS(config)# rlog-file send compress zip
```

3. The following example configures the JSON format for RLOG files.

```
FS(config)# rlog-file send format elog
```

Verification

Run the **show rlog-file** command to display values of the RLOG file export parameters.

1.13 rlog-file server

Use this command to configure the RLOG file server.

Use the **no** form of this command to cancel the RLOG file server.

rlog-file server *protocol ip-address* [**port** *port-num*] [**oob**] [**path** *server-path-string*] [**username** *username-string* **passwd** *passwd-string*]

no rlog-file server

Parameter Description

Parameter	**Description**
protocol	Protocol (FTP or HTTP)
ip-address	IP address of the RLOG file server
port-num	Service port of the RLOG file server. This port is applicable only in HTTP mode. The default port is Port 80.
oob	OOB interface, available only in HTTP mode
server-path-string	Server path. The default path is **l**.
username-string	Username. The default value is **FS**.
passwd-string	Password. The default value is **FS**.

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

An RLOG file server must be configured to export RLOG files.

⚠ Currently, only one RLOG file server is supported. A later configuration overwrites an earlier one.

Configuration Examples

The following example configures an RLOG file server compliant with FTP.

```
FS(config)# rlog-file server 10.10.10.2 path rlog/ username test passwd test
```

Verification

Run the **show rlog-file** command to check whether the server information is consistent.

1.14 rlog-file storage

Use this command to configure the size of the local storage for RLOG files.

Use the **no** form of this command to restore the size of the local storage for RLOG files to the default value.

rlog-file storage *storage-size*

no rlog-file storage

Parameter Description

Parameter	Description
storage-size	Size (in KB) of the local storage for RLOG files

Defaults

By default, the size of the local storage for RLOG files is 65,536 KB in real-time mode and is 1,048,576 KB in scheduled mode.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Set the size of the local storage for RLOG files according to the actual storage space of the RLOG device.

Configuration Examples

The following example sets the size of the local storage to 2,097,152 KB.

```
FS(config)# rlog-file storage 2097152
```

Verification

Run the **show rlog** command to display the size of the local storage for RLOG files.

1.15 rlog-file type

Use this command to configure the RLOG file type.

Use the **no** form of this command to cancel the RLOG file type.

rlog-file type *type-num*

no rlog-file type *type-num*

Parameter Description

Parameter	Description
type-num	RLOG file type

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide The RLOG file type must be configured to enable RLOG file export.

⚠ If this command is disabled, RLOG files are not exported.

Configuration Examples The following example configures URL audit log export in file mode.

```
FS(config)# rlog-file type 20
```

Verification Run the **show rlog** command to display the RLOG file type.

1.16 show nat-log

Use this command to display NAT logging information.

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*

Parameter Description

Parameter	Description
user_name	Username
ip-protocol	Protocol ID
source-ip	Source IP address
dst-ip	Destination IP address
src-port	Source port ID, ranging from **0** to **65535**
dst-port	Destination port ID, ranging from **0** to **65535**
begin-year	Start year, ranging from **1993** to **2035**
begin-mon	Start month, ranging from **1** to **12**
begin-day	Start day, ranging from **1** to **31**
begin-hour	Start hour, ranging from **0** to **23**
end-year	End year, ranging from **1993** to **2035**
end-mon	End month, ranging from **1** to **12**
end-day	End day, ranging from **1** to **31**
end-hour	End hour, ranging from **0** to **23**

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to display flow/NAT logs in a specific period by username, protocol ID, source IP address, source port, destination IP address, and destination port.

Configuration Examples The following example displays logs generated from 03:00 to 05:00 on October 06, 2010.

```
FS#show nat-log time-interval 2010 10 6 3 t 2010 10 6 5
count:427
Pr   SrcAddr                              DstAddr                              UserName
SrcPort        DstPort        Vrf          SendBytes   RecvBytes   time
17   192.168.122.62 (0.0.0.0)            192.168.122.255(0.0.0.0)           192.168.122.62
138   (0)       138   (0)       0          2028          0            2010-10-6 3:1
17   192.168.100.55 (0.0.0.0)            192.168.100.255(0.0.0.0)           192.168.100.55
138   (0)       138   (0)       0          732           0            2010-10-6 3:1
17   192.168.122.54 (0.0.0.0)            192.168.122.255(0.0.0.0)           192.168.122.54
137   (0)       137   (0)       0          864           0            2010-10-6 3:1
138   (0)       138   (0)       0          714           0            2010-10-6 3:3
```

Field description

Field	Description
Pr	Protocol
SrcAddr	Source address
DstAddr	Destination address
UserName	Username
SrcPort	Source port
DstPort	Destination port
Vrf	VRF name
RecvBytes	Number of received bytes
time	Flow time

Gateway products do not support VRF. The preceding configuration example is for reference only.

1.17 show rlog

Use this command to display the RLOG configuration information.

show rlog

Parameter Description

Parameter	Description
N/A	*N/A*

Command Mode Privileged EXEC mode

Default Level

14

Usage Guide

This command can display information about the RLOG server, such as the local IP address of the RLOG device, export rate, exported log count, and RLOG combination configuration.

Configuration Examples

The following example displays the RLOG configuration information.

```
FS#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 1000 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
```

Field description

Field	Description
rlog server is enable	Indicates that the RLOG server is enabled.
rlog dev-ip	Local IP address of the RLOG device
rlog export-rate	RLOG export rate
rlog queue remain	Number of remaining nodes of RLOG
send log count	Number of exported logs
error count	Number of logs that failed to be exported
errorno	Error code of the last export failure
recv buf	Number of logs received by RLOG
poll buf err	RLOG cache space insufficiency count
local buf	Local log output count
recv err cnt	Received message error count
depatch err cnt	Number of received messages that have no corresponding servers or whose corresponding servers are ineffective
enable log combination	Specifies whether to enable RLOG combination for export.

1.18 show rlog-file

Use this command to display the RLOG file mode configuration information.

show rlog-file

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command can display the RLOG file server information, such as the log storage path, size of the log storage directory, RLOG type, and RLOG export parameters.

Configuration Examples

The following example displays the RLOG file configuration information.

```
FS#show rlog-file
rlog file server ftp:
      ip:10.10.10.2, port:21 oob
      path: rlog/
      username:ftp    passwd:ftp
local path: /tmp/rlog-file
local storage: 65536 K
send time-rage: from 22 to 6
send compress: zip; format: json
total proc files: 99
client count: 2
log             total   tar|err   send|err   lasterr
LOG              100     100|0     100|0       0
MAIL_BODY        100     100|0     100|0       0
MAIL_ATTACH      100     100|0     100|0       0
WEBMAIL          100     100|0     100|0       0
BSS_BODY         100     100|0     100|0       0

send log type:
RLOG_FILE_TYPE_URL_AUDIT    20
```

Field description

Field	Description
ip	Server IP address
port	Server port
oob	Management interface for export
path	Server export path
username	Username for accessing the server
passwd	Password for accessing the server
local path	Local storage path
local storage	Local storage size limit
send time-rage	Time range for scheduled export
send protocol	RLOG export protocol
total proc files	Number of processed RLOG files
client count	Client count

tar file error	Number of file compression errors and code of the last error
put file error	Number of file export errors and code of the last error
send log type	RLOG type

1.19 show rlog-status

Use this command to display the status of the RLOG server.

show rlog-status { [**server** *ip*] | [**client**] | [**log**] }

Parameter Description

Parameter	Description
Ip	IP address of the RLOG server

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command can display the status of the RLOG server.

Configuration Examples

1. The following example displays information about all RLOG servers.

```
FS#show rlog-status
============================================================
server:192.168.1.100       port:20000
type                                   prio
============================================================
server:10.10.10.10        port:20000
type                                   prio
RLOG_TYPE_FLOW          16          1
```

Field description

Field	Description
server	Server address
port	Server port
type	RLOG type supported by the server
prio	RLOG priority of the server

2. The following example displays the number of clients connected to RLOG.

```
FS#show rlog-status client
rlog client count: 0
```

Field description

Field	Description
rlog client count	Number of clients connected to RLOG

3. The following example displays the number of logs received by RLOG.

```
FS#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
```

Field description

Field	Description
local rlog message	Number of received local logs of RLOG
remote rlog message	Number of received remote logs (differentiated by RLOG type) of RLOG

1.20 show rlog-type

Use this command to display supported RLOG types.

show rlog-type

Parameter Description

Parameter	Description
N/A	*N/A*

Command Mode

Privileged EXEC mode

Default Level 14

Usage Guide This command can display supported RLOG types.

Configuration Examples The following example displays supported RLOG types.

```
FS#show rlog-type
RLOG_TYPE_FLOW                    16
RLOG_TYPE_CPU_MEM                 17
RLOG_TYPE_DISC                    18
RLOG_TYPE_DEV_LOG                 19
RLOG_TYPE_URL_AUDIT               20
RLOG_TYPE_SESSION                 21
RLOG_TYPE_IP_APP                  22
RLOG_TYPE_IP                      23
RLOG_TYPE_CHANNEL                 24
RLOG_TYPE_INTERFACE               25
RLOG_TYPE_IP_OFFLINE              26
RLOG_TYPE_MAIL_AUDIT              27
RLOG_TYPE_TELNET_AUDIT            28
RLOG_TYPE_WEB_SEARCH_AUDIT        29
RLOG_TYPE_WEB_BBS_AUDIT           30
RLOG_TYPE_IM_AUDIT                31
RLOG_TYPE_FTP_AUDIT               32
RLOG_TYPE_WEB_AUDIT               33
RLOG_TYPE_APP_AUDIT               34
RLOG_TYPE_FLOOD                   35
RLOG_TYPE_FLOOD_CEASEm            36
RLOG_TYPE_SCAN                    37
RLOG_TYPE_SCAN_CEASE              38
RLOG_TYPE_ATTACK_FRAG             39
```

Field description

Field	Description
N/A	The parameters are displayed in the format of RLOG type name + RLOG type value.

2 POLICE-LOG Commands

2.1 content-audit write-plog

Use this command to enable content audit log monitoring.

[**no**] **content-audit write-plog {***im* | *mail* | *url* | *vid* | *web-bbs* | *web-mail* | *web-search***}**

Use the **no** form of this command to disable the content audit log monitoring.

[**no**] **content-audit write-plog {***im* | *mail* | *url* | *vid* | *web-bbs* | *web-mail* | *web-search***}**

Parameter Description

Parameter	Description
im	Enables IM chat log sending to POLICE-LOG.
mail	Enables client mail log sending to POLICE-LOG.
url	Enables HTTP log sending to POLICE-LOG.
vid	Enables virtual identity audit sending to POLICE-LOG.
web-bbs	Enables Web BBS log sending to POLICE-LOG.
web-mail	Enables Web mail log sending to POLICE-LOG.
web-search	Enables Web search log sending to POLICE-LOG.

Defaults

The content audit log monitoring is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable content audit log sending to POLICE-LOG.

Configuration Example

#Enable content audit log sending to POLICE-LOG.

```
FS(config)#content-audit write-plog ?
  im            Im audit information
  mail          Mail audit information
  url           Url audit information
  vid           Vid audit information
  web-bbs       Web-bbs audit information
  web-mail      Web-mail audit information
  web-search    Web-search audit information

FS(config)#content-audit write-plog
```

Verification

Run the **show content-audit plog config** command to display the configuration status.

2.2 debug police-log

Use this command to enable log debugging of a specified log level.

debug police-log {*auth* | *common* | *mail* | *nat* | *setdev* | *url* | *vid* | *webbbs* | *websearch***}**

Use the **no** form of this command or the **undebug police-log** command to restore the default log level.

no debug police-log {*auth* | *common* | *mail* | *nat* | *setdev* | *url* | *vid* | *webbbs* | *websearch*}

or

undebug police-log {*auth* | *common* | *mail* | *nat* | *setdev* | *url* | *vid* | *webbbs* | *websearch*}

Parameter Description

Parameter	Description
-auth	Enables authentication log debugging.
-common	Enables debugging on the five types of content audit logs.
-getdev	Enables debugging on obtained location information.
-mail	Enables mail log debugging.
-nat	Enables NAT log debugging.
-setdev	Enables debugging on obtained heartbeat information.
-url	Enables HTTP log debugging.
-vid	Enables virtual identity log debugging.
-webbbs	Enables Web BBS log debugging.
-websearch	Enables Web search log debugging.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is a debugging switch for troubleshooting. For example, the Managed @ Cloud Center shows that a device goes offline; in this case, you can enable logging to display detailed interaction data in POLICE-LOG.

⚠ Enable the **log on** and **log console** commands before using the _syslog module to output debugging logs.

Configuration Example

#Enable log debugging.

```
FS#debug police-log ?
  auth            Open auth police log debug
  common            Open all common police log debug
  getdev          Open get dev status debug
  mail            Open mail police log debug
  nat             Open nat police log debug
  setdev          Open set dev status debug
  url             Open url police log debug
  vid             Open vid police log debug
  webbbs            Open webbbs police log debug
websearch   Open websearch police log debug
```

#Disable log debugging.

```
FS#no debug police-log ?
  auth            Open auth police log debug
```

```
common      Open all common police log debug
getdev      Open get dev status debug
mail        Open mail police log debug
nat         Open nat police log debug
setdev      Open set dev status debug
url         Open url police log debug
vid         Open vid police log debug
webbbs      Open webbbs police log debug
websearch   Open websearch police log debug
```

Debugging

3. #Request MACC for location information.

Debugging Information	https://192.168.23.206/specification/service/dc/getDevConf post data:{"device_sn":"1234842571023", "device_mac":"00-D0-F8-22-35-35", "device_type":0}
Description	The local device requests for location information.
Cause	The request for location information is triggered by a device startup or a periodic update of the location information.
Handling Suggestion	N/A

4. #Request for heartbeat connections.

Debugging Information	https://192.168.23.206/specification/service/ds/setDevStatus
	post data:{"netbar_wacode":"35011110341520","collection_equipment_id": "75496176400D0F8223535", "device_status":"00"}
	{"code":0,"msg":"ok"}

Description	The local device sends heartbeat request packets.
Cause	The sending of heartbeat request packets is triggered by periodical heartbeats.
Handling Suggestion	N/A

5. #Report logs.

Debugging Information	https://120.35.11.138:4433/specification/service/fileUpload?collection_equipment_id= 754961764FFFFFFFFFFFF&line_count=31 /tmp/log//145-010000-1456709687-00000-WA_SOURCE_FJ_0001-0.xml {"code":"0","msg":"ok"}
Description	The local device sends logs.
Cause	Log sending is triggered by the requirement of the local device for actively uploading logs of a location.

Handling Suggestion	N/A

Verification Run the **show debugging** command to display the configuration status.

2.3 nat-log police

Use this command to enable NAT flow log audit.

nat-log police

Use the **no** form of this command to disable NAT flow log audit.

no nat-log police

Parameter Description

Parameter	Description
N/A	N/A

Defaults The NAT flow log audit is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable NAT flow log monitoring.

Configuration Example #Enable POLICE-LOG.

```
FS# configure
FS(config)# nat-log police
FS(config)# exit
FS# wr
```

Verification Run the **show nat-log status** command to display the configuration status.

2.4 police-log enable

Use this command to enable POLICE_LOG.

police-log enable

Use the **no** form of this command to disable POLICE_LOG.

no police-log enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults POLICE_LOG is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable POLICE-LOG, which sends corresponding logs.

Configuration Example

#Enable POLICE-LOG.

```
FS# configure
FS(config)# police-log enable
FS(config)# exit
FS# wr
```

Verification

Run the **show police-log config** command to display the configuration status.

2.5 police-log file-sender compress

Use this command to enable the log compression function of POLICE_LOG.

police-log file-sender compress

Use the **no** form of this command to disable the log compression function of POLICE_LOG.

no police-log file-sender compress

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The log compression function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to compress or decompress logs sent to the ELOG server.

Configuration Example

#Enable the network monitoring log compression function.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#police-log file-sender compress
FS(config)#
FS# wr
```

Verification

Run the **show police-log config** command to display the configuration status.

2.6 police-log set url

Use this command to set the URL to ELOG server. police-log set url *url*

Use the **no** form of this command to clear the URL for ELOG server. **no police-log set url**

Parameter

Parameter	Description

Description

url	Indicates the complete URL for accessing the homepage of the ELOG system. Check whether the ELOG server is located in the same sub directory of the server.

Defaults No URL is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to configure the URL of the ELOG server. Note that the URL must be a complete URL of the ELOG server as multiple sets of Web services may be deployed on some servers.

Configuration Example #Configure the URL

```
 FS# configure
FS(config)# police-log set url https://172.18.124.35/specification/
FS(config)# exit
FS# wr
```

Verification Run the **show police-log config** command to display the configuration status.

2.7 police-log set platform

Use this command to configure an interconnection platform.

police-log set platform { **elog** | { *platform-type* [**name** *plat-name*] } }

Use the **no** form this command to clear the configuration of the interconnection platform.

no police-log set platform { **elog** | { *platform-type* [**name** *plat-name*] } }

Sub Command

[**no**] { **data-gather | send-para** } *key-string value*

Parameter Description

Parameter	**Description**
platform-type	elog: Indicates that the ELOG server is interconnected. surfilter: Indicates that the Surfilter system is interconnected.
plat-name	Platform name.
data-gather	Configures data gathering.
send-para	Configures data sending.
key-string	You can get the key-string by running the following two commands” **show plog para-list data-gather** *plat-name* **show plog para-list send-para** *palt-name*
value	Value

Defaults Elog is interconnected by default.

Command Mode Global configuration mode

Default Level 15

Usage Guide Use this command to configure an interconnection platform.

Configuration Example #Configure Elog as interconnection platform.

```
FS# configure
FS(config)# police-log set platform elog
FS(config)# end
FS# wr
```

#Configure Surfilter as interconnection platform.

```
FS# configure
FS(config)# police-log set platform surfilter renzixing
FS(config)# end
FS# wr
```

Verification Run the **show run** command to display the configuration status.

Prompt N/A

Common Errors N/A

Platform Description This command is supported by the EG and NBR (except CS) series but not the MSC, NBR-C/S, and AG and ACE products.

2.8 netsite

Use this command to set a netsite.

netsite *index*

Sub Command: **service-name** | **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**

Use this command to remove the configuration.

no netsite

Parameter

Parameter	Description

Description

index	Sets an index.

Defaults

No netsite is set by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Example

#Set a netsite.

```
FS# configure
FS(config)# netsite 1
FS(config-netsite)# end
FS# wr
```

2.9 police-log set security-org-code

Use this command to set the security organization code.

police-log set security-org-code *code*

Use the **no** form of this command to remove the configuration.

no police-log set security-org-code

Parameter Description

Parameter	Description
code	Sets a security organization code.

Defaults

No security organization code is set by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Example

#Set a security organization code.

```
FS# configure
FS(config)# police-log set security-org-code 756461674
FS(config)# end
FS# wr
```

2.10 police-log set collection-type

Use this command to set a collection type.

police-log set collection-type *type*

Use the **no** form of this command to remove the configuration.

no police-log set collection-type

Parameter Description

Parameter	Description
type	Set a collection type.

Defaults No collection type is set by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example #Set a collection type.

```
FS# configure
FS(config)# police-log set collection-type 1
FS(config)# end
FS# wr
```

2.11 police-log set source-wacode

Use this command to set a source code.

police-log set source-wacode *code*

Use the **no** form of this command to remove the configuration.

no police-log set source-wacode

Parameter Description

Parameter	Description
code	Sets a source code.

Defaults No source code is set by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example #Set a source code..

```
FS# configure
FS(config)# police-log set source-wacode 123456
FS(config)# end
FS# wr
```

2.12 police-log set destination-wacode

Use this command to set a destination code.

police-log set source-wacode *code*

Use the **no** form of this command to remove the configuration.

no police-log set source-wacode

Parameter Description

Parameter	Description
code	Sets a destination code.

Defaults No destination code is set by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example #Set a destination code.

```
FS# configure
FS(config)# police-log set destination-wacode 123456
FS(config)# end
FS# wr
```

2.13 police-log set org-name

Use this command to set an organization name.

police-log set org-name *name*

Use the **no** form of this command to remove the configuration.

no police-log set org-name

Parameter Description

Parameter	Description
name	Sets an organization name.

Defaults No organization name is set by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example #Set an organization name.

```
FS# configure
FS(config)# police-log set org-name FS
FS(config)# end
FS# wr
```

2.14 police-log set org-address

Use this command to set an organization address.

police-log set org-address *address*

Use the **no** form of this command to remove the configuration.

no police-log set org-address

Parameter Description

Parameter	Description
address	Sets an organization address.

Defaults No organization address is set by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example

#Set an organization address.

```
FS# configure
FS(config)# police-log set org-address test
FS(config)# end
FS# wr
```

2.15 police-log set org-person

Use this command to set an organization contact person.

police-log set org-person *person*

Use the **no** form of this command to remove the configuration.

no police-log set org-person

Parameter Description

Parameter	Description
person	Sets an organization contact person.

Defaults No contact person is set by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example

#Set an organization contact person.

```
FS# configure
FS(config)# police-log set org-person Alice
FS(config)# end
FS# wr
```

2.16 police-log set org-tel

Use this command to set an organization phone number.

police-log set org-tel *phone*

Use the **no** form of this command to remove the configuration.

no police-log set org-tel

Parameter Description

Parameter	**Description**
phone	Sets an organization phone number.

Defaults No organization phone number is set by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example

#Set an organization phone number.

```
FS# configure
FS(config)# police-log set org-tel 13300000000
FS(config)# end
FS# wr
```

2.17 police-log set org-mail

Use this command to set an organization mail.

police-log set org-mail *mail*

Use the **no** form of this command to remove the configuration.

no police-log set org-mail

Parameter Description

Parameter	**Description**
mail	Sets an organization mail.

Defaults No organization mail is configured by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example

#Set an organization mail.

```
FS# configure
FS(config)# police-log set org-mail 123@163.com
FS(config)# end
FS# wr
```

2.18 police-log set ftp server

Use this command to set an FTP server.

police-log set ftp server *url* **source [interface** *interface-name* **|** *addr* **]**

Use the **no** form of this command to remove the configuration.

no police-log set ftp

Parameter Description

Parameter	Description
url	Sets a URL.
interface-name	Sets an interface.
addr	Set a local IP address.

Defaults Not FTP server is configured by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example #Set an FTP server.

```
FS# configure
FS(config)# police-log set ftp server 127.0.0.1:21 source interface gi 0/1
FS(config)# exit
FS# wr
```

2.19 police-log set ftp username

Use this command to set an FTP username and password.

police-log set ftp username *user* **password pass**

Use the no form of this command to remove the configuration.

no police-log set ftp username

Parameter Description

Parameter	Description
user	Sets an FTP username.
pass	Sets an FTP password.

Defaults No FTP username or password is configured by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example #Configure an FTP username and password.

```
FS# configure
FS(config)# police-log set ftp username test password test
FS(config)# exit
FS# wr
```

2.20 police-log add ap

Use this command to configure an AP.

police-log add ap { **apmac** | **apname** | **aptype** | **apfloor** | **service-code** | **create-time** }

Use the no form of this command to remove the configuration.

[**no**] **police-log add ap apmac**

Parameter Description

Parameter	Description
apmac	Sets an AP MAC address.
apname	Sets an AP name.
aptype	Sets an AP type.
apfloor	Sets a floor.
service-code	Sets a service code.
create-time	Sets a time.

Defaults No AP is configured by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example

#Configure an AP.

```
FS# configure
FS(config)# police-log add ap apmac 00-11-44-77-22-55 apname testap aptype 0 apfloor 2f service-code 11111111111111 create-time 2000-01-01
FS(config)# exit
FS# wr
```

2.21 show police-log config

Use this command to display the configuration information of the POLICE-LOG.

show police-log config

Parameter Description

Parameter	Description
N/A	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, check whether POLICE-LOG is enabled and whether POLICE-LOG is successfully interconnected.

Configuration Example

#Display the configuration information of POLICE-LOG.

```
FS#show police-log config
police log configuration
    >police log: enable
    >server url: https://192.168.25.184:443/specification
    >auth type: define (1021999)
>file compress: enable
```

Field description:

Field	Description
police-log	Specifies the status of POLICE-LOG. This field can be set to **enable** or **disable**.
server url	Specifies the URL of the ELOG server.
auth type	Specifies the authentication type.
file compress	Specifies the compression switch. This field can be set to **enable** or **disable**.

2.22 show police-log status

Use this command to display the running status of POLICE-LOG.

show police-log status

Parameter Description

Parameter	Description
N/A	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, check whether POLICE-LOG is enabled and whether POLICE-LOG is successfully interconnected.

Configuration Example

#Display the running status of POLICE-LOG.

```
FS#show police-log status
-------------police-log status--------------
>police-log:        enable
>server status:    connected
>log total deal: 2626      speed:0
>file total send:184       failed:16           waiting:0
>compress:              disable
-------------AUTH LOG---------------
in>      rcv:2,        deal:2,    fail:0
out>     rcv:2,        deal:2,    fail:0
file> send:1,         fail:3,                drop:1
-------------NAT LOG---------------
in>      rcv:2568, deal:2568,             fail:0
out>     rcv:2568, deal:2568,             fail:0
```

```
file> send:141,    fail:50,            drop:13
-------------VID LOG---------------
in>     rcv(vid):0,            deal:0,    fail:0
out>    rcv(vid+im):19,     deal:19,               fail:0
file> send:15,      fail:5,              drop:1
-------------URL LOG---------------
out>    rcv:37,      deal:37,               fail:0
file> send:11,      fail:7,              drop:1
-------------MAIL LOG---------------
out>    rcv:0,       deal:0,    fail:0
file> send:0,       fail:0,              drop:0
-------------WEBBBS LOG---------------
out>    rcv:0,       deal:0,    fail:0
file> send:0,       fail:0,              drop:0
-------------WEBSEARCH LOG---------------
out>    rcv:0,       deal:0,    fail:0
file> send:0,       fail:0,              drop:0
```

Field description:

Field	Description
police-log	Specifies the status of POLICE-LOG. This field can be set to **enable** or **disable**.
server status	Specifies whether it is connected. This field can be set to **connected** or **disconnect**.
log total deal	Specifies the total number of processed logs and the processing speed.
file total send	Specifies the total number of sent logs and the number of logs failed to be sent.
compress	Specifies the compression switch. This field can be set to **enable** or **disable**.
AUTH LOG	Specifies the authentication log statistics.
NAT LOG	Specifies NAT log statistics.
VID LOG	Specifies virtual identity log statistics.
URL LOG	Specifies HTTP log statistics.
MAIL LOG	Specifies mail log statistics.
WEBBBS LOG	Specifies Web BBS log statistics.
WEBSEARCH LOG	Specifies Web search log statistics.

3 LOG-POLICY Commands

3.1 log-policy

Use this command to configure a log policy based on the user name. Use the **no** form of this command to delete a log policy.

log-policy *policy-name* { **netlog | 82log | none** }

no log-policy *policy-name*

Parameter Description

Parameter	Description
policy-name	Indicates the log policy name, which is a string of a maximum of 64 bytes.

Defaults

No log policy is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1. Log policies must have unique names.
2. A maximum of 1,000 log policies can be configured.

Configuration Examples

The following example adds a log policy.

```
FS# configure terminal
FS(config)# log-policy eg 82log
FS(config)#end
```

The following example deletes a log policy.

```
FS# configure terminal
FS(config)#no log-policy eg
FS(config)# end
```

Verification

Run the **show running-config** command to display the configuration.

Prompt Message

1. A prompt appears when the log policy name exceeds the maximum length.

```
FS(config)#log-policy kkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk netlog username
zd 3
invalid policyname, the maximum length of policyname is 64!
```

2. A prompt appears when the number of log policies exceeds the limit.

```
FS(config)#log-policy k1001 netlog
The maximum capacity has been reached, the max number of log policy is 1000!
```

3.2 log-policy-relate

Use this command to set the object associated with a log policy. Use the **no** form of this command to delete the object associated with a log policy.

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-subscriber** *user-name* }

no 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-subscriber** *user-name* }

Parameter Description

Parameter	Description
policy-name	Indicates the log policy name, which is a string of a maximum of 64 bytes.
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, which is a string of a maximum of 128 bytes.

Defaults

No object is associated with a log policy by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1. When a log policy with the same name as an existing log policy is configured, the existing log policy is modified.
2. When an IP range is configured, the start IP address must be smaller than the end IP address.
3. Each IP-based log policy can associate with only one object.
4. 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 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 Examples

The following example associates a log policy with a static user.

```
FS# configure terminal
FS(config)# log-policy-relate relate policyname sub-any subscriber any
FS(config)#end
```

The following example associates a log policy with a dynamic user.

```
FS# configure terminal
FS(config)# log-policy-relate relate policyname auth auth-subscribe any
FS(config)#end
```

The following example associates a log policy with an IP address.

```
FS# configure terminal
FS(config)# log-policy-relate relate policyname ip ip-host 192.168.3.11
FS(config)# end
```

The following example associates a log policy with an IP subnet.

```
FS# configure terminal
FS(config)# log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0
FS(config)#end
```

The following example associates a log policy with an IP range.

```
FS# configure terminal
FS(config)# log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1
FS(config)# end
```

Verification

Run the **show running-config** command to display the configuration.

Prompt Message

1. A prompt appears when the number of log policies exceeds the limit.

```
FS(config)#log-policy k1001 netlog
The maximum capacity has been reached, the max number of log policy is 1000!
```

2. A prompt appears if the start IP address is greater than the end IP address for a log policy configured based on the IP range.

```
FS(config)#log-policy policyname kk netlog ip-range 192.168.2.1 192.168.1.1 2
invalid param, 192.168.2.1 must greater than 192.168.1.1
```

3.3 log-policy-config

Use this command to change the priorities of two log policies.

log-policy-config priority-swap *policy-name1 policy-name2*

Parameter Description

Parameter	**Description**
policy-name1	Indicates the log policy name, which is a string of a maximum of 64 bytes.
policy-name2	Indicates the log policy name, which is a string of a maximum of 64 bytes.

Defaults

Log policy priority change is not configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1. The log policies whose priorities need to be changed must exist.
2. The two policies must be in sequence in the command.

Configuration Example

The following example changes the priorities of two log policies.

```
FS# configure terminal
FS(config)# log-policy-config priority-swap subnet range
FS(config)# end
```

Verification

Run the **show running-config** command to display the configuration.

Prompt Message

A prompt appears if the log policies whose priorities need to be changed do not exist.

```
FS(config)# log-policy-config priority-swap subnet xx
swap failed
```

3.4 show log-policy

Use this command to display log policy information.

show log-policy [**policyname** *policy-name*]

Parameter Description

Parameter	Description
policy-name	Indicates the log policy name, which is a string of a maximum of 64 bytes.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

When no policy name is specified, information about all log policies is displayed. When a policy name is specified, information about the specific log policy is displayed.

Configuration Examples

The following example displays all log policies.

```
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
```

The following example displays the log policy with the name specified.

```
FS# show log-policy policyname ip
   log-policy ip none
         log-policy-relate relate policyname ip ip-host 192.168.3.11
```

Prompt Message

A prompt appears when the log policy name exceeds the maximum length.

```
FS(config)#show log-policy kkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk
invalid policyname, the maximum length of policyname is 64!
```

3.5 clear log-policy

Use this command to delete all log policies.

clear log-policy

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example deletes all log policies.

```
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# clear log-policy
FS# show log-policy

FS#
```

Prompt

A prompt appears when the log policy name exceeds the maximum length.

Message

4 SNMP Commands

4.1 clear snmp locked-ip

Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures.

clear snmp locked-ip [**ipv4** *ipv4-address*]

Parameter Description

Parameter	Description
ipv4 *ipv4-address*	Clears a specified IPv4 address.

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures. You can clear the whole source IP address table or a specific source IP address.

After the source IP addresses locked are cleared, the SNMP packets with these source IP addresses could be authenticated again.

Configuration Examples

The following example clears the whole source IP address table locked after continuous SNMP authentication failures.

```
FS#clear snmp locked-ip
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.2 no snmp-server

Use this command to disable the SNMP agent function.

no snmp-server

Parameter Description

Parameter	Description
N/A	N/A

Defaults

SNMP agent is enabled by default.

Command mode

Global configuration mode.

Usage Guide

This command disables the SNMP agent services of all versions supported on the device.

Configuration Examples

The following example disables the SNMP agent.

```
FS(config)# no snmp-server
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.3 show snmp

Use this command to display the SNMP configuration.

show snmp [**mib** | **user** | **view** | **group** | **host | locked-ip | process-mib-time**]

Parameter Description

Parameter	Description
mib	Displays the SNMP MIBs supported.
user	Displays the SNMP user information.
view	Displays the SNMP view information.
group	Displays the SNMP user group information.
host	Displays the explicit host configuration.
locked-ip	Displays the source IP addresses locked after continuous SNMP authentication failures.
process-mib-time	Displays the MIB node requiring the longest processing time.

Defaults

N/A

Command mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The example below displays the SNMP configuration:

```
FS# show snmp
Chassis: 60FF60
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: disabled
SNMP logging: disabled
SNMP agent: enabled
```

Related Commands

Command	Description
snmp-server chassis-id	Specifies the SNMP system sequence number.

Platform Description

N/A

4.4 snmp trap link-status

Use this command to enable the interface to send link traps. Use the **no** form of this command to disable the interface to send link traps.

snmp trap link-status

no snmp trap link-status

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Sending link traps on the interface is enabled by default. If the interface link status changes, SNMP link traps will be sent.

Command mode

Interface configuration mode

Usage Guide

This command can be configured on the Ethernet interface, aggregate ports and SVI interfaces.

Configuration Examples

The following example disables the interface to send link traps.

```
FS(config)# interface gigabitEthernet 1/1
FS(config-if–GigabitEthernet 1/1)# no snmp trap link-status
```

The following example enables the interface to send link traps.

```
FS(config)# interface gigabitEthernet 1/1
FS(config-if–GigabitEthernet 1/1)# snmp trap link-status
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.5 snmp-server authentication attempt

Use this command to configure the maximum number of continuous SNMP authentication failures, and specified the action policy for the authentication failure. Use the **no** form of this command to remove the limit of continuous SNMP authentication failures and the related action policies.

snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

no snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

Parameter Description

Parameter	Description
times	The maximum number of continuous SNMP authentication failures. The range is from 1 to 10.
exceed	Indicates the action policy in the case that the maximum number of continuous SNMP authentication failures is exceeded.
lock	Indicates that the source IP address is permanently locked to be authenticated and can be unlocked only by the administrator's manual configuration.
lock-time *minutes*	Indicates that the source IP address is locked for a period of time. The *minutes* indicates the lock time, ranging from 1 to 65,535. The unit is minute.
unlock	Indicates that no action policy is configured for the authentication failed user, that is, the SNMP authentication for this user is allowed.

Defaults

SNMP attack prevention is disabled by default.

Command mode

Global configuration mode

Usage Guide

The IP address of the SNMP authentication failed user is added to the blacklist. When the maximum number of continuous SNMP authentication failures is exceeded, the system will perform the related authentication limit actions according the configured policy:

1. For the permanently locked IP addresses: The source IP addresses can be authenticated only after the administrator unlock them manually.
2. For the IP addresses locked for a period time: The source IP addresses can be authenticated only after the lock time expires or the administrator unlock them manually.
3. For the unlocked IP addresses: The source IP address can pass the authentication as long as the correct community (for SNMPv1 and SNMPv2) or username (for SNMPv3) is used.

Configuration Examples

The following example configures the maximum number of continuous SNMP authentication failures to 4, and sets the IP address lock time to 30 seconds.

```
FS(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.6 snmp-server chassis-id

Use this command to specify the SNMP chassis ID. Use the **no** form of this command to restore the default chassis ID.

snmp-server chassis-id *text*

no snmp-server chassis-id

Parameter Description

Parameter	Description
text	SNMP chassis ID: numerals or characters.

Defaults

The default is 60FF60.

Command mode

Global configuration mode.

Usage Guide

The SNMP chassis ID is generally the serial number of the device to facilitate identification. The SNMP chassis ID can be displayed through the **show snmp** command.

Configuration Examples

The following example specifies the SNMP chassis ID as 123456:

```
FS(config)# snmp-server chassis-id 123456
```

Related Commands

Command	Description

show snmp	Displays the SNMP configuration.

Platform Description N/A

4.7 snmp-server community

Use this command to specify the SNMP community access string. Use the **no** form of this command to remove the SNMP community access string.

snmp-server community [0 | 7] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*] [*aclnum*] [*aclname*]

no snmp-server community [0 | 7] *string*

Parameter Description

Parameter	Description
0	Indicates that the community string is in plaintext.
7	Indicates that the community string is in ciphertext.
string	Community string, which is the communication password between the NMS and the SNMP agent
view-name	View name
ro	Indicates that the NMS can only read the variables of the MIB.
rw	Indicates that the NMS can read and write the variables of the MIB.
aclnum	Access list number (1 to 199, and 1300 to 2699), which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Access list name, which specifies the IPV4 addresses that are permitted to access the MIB.
ipaddr	Specifies the IP address of the NMS to access the MIB.

Defaults All communities are read only by default.

Command mode Global configuration mode.

Usage Guide This command is an essential command to enable the SNMP agent function, such as specifying the community attribute and IP addresses of NMS to access the MIB.

To disable the SNMP agent function, use the **no snmp-server** command.

Configuration Examples The following example defines a SNMP community access string named public, which can be read-only.

```
FS(config)# snmp-server community public ro
```

Related Commands

Command	Description
access-list	Defines an access list.

Platform N/A

Description

4.8 snmp-server contact

Use this command to specify the system contact string. Use the **no** form of this command to remove the system contact string.

snmp-server contact *text*

no snmp-server contact

Parameter Description

Parameter	Description
text	Defines a system contact string.

Defaults No system contact string is set by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies the SNMP system contract i-net800@i-net.com.cn:

```
FS(config)# snmp-server contact i-net800@i-net.com.cn
```

Related Commands

Command	Description
show snmp-server	Displays the SNMP configuration.
no snmp-server	Disables the SNMP agent function.

Platform Description N/A

4.9 snmp-server enable secret-dictionary-check

Use this command to enable the secret dictionary check for the **community** and **user** fields. Use the **no** form of this command to disable the secret dictionary check.

snmp-server enable secret-dictionary-check

no snmp-server enable secret-dictionary-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults Secret dictionary check for the **community** and **user** fields is disabled by default.

Command mode Global configuration mode.

Usage Guide This command must be used together with the **password policy** command.

Configuration Examples The following example enables the secret dictionary check for the **community** field.

```
FS(config)# password policy min-size 6
FS(config)# snmp-server enable secret-dictionary-check
FS(config)#snmp-server community abc12
% The community(abc12) is a weak community!
```

Related Commands

Command	Description
snmp-server host	Specifies the SNMP host to send the SNMP trap message.

Platform Description N/A

4.10 snmp-server enable traps

Use this command to enable the SNMP agent to send the SNMP trap massage to NMS. Use the **no** form of this command to disable the SNMP agent to send the SNMP trap massage to NMS.

snmp-server enable traps [*notification-type*]

no snmp-server enable traps

Parameter Description

Parameter	Description
notification-type	Specifies the type of trap messages. snmp: SNMP trap message bridge: Bridge trap message. mac-notification: MAC trap message. ospf: OSPF trap message. vrrp: VRRP trap message. web-auth: Web authentication trap message.

Defaults Sending trap message to the NMS is disabled by default.

Command mode Global configuration mode.

Usage Guide This command must be used together with the **snmp-server host** command to send the trap message. Specifying no trap type indicates all trap messages are sent.

Configuration Examples The following example enables the SNMP agent to send the SNMP trap message.

```
FS(config)# snmp-server enable traps snmp
FS(config)# snmp-server host 192.168.12.219 public snmp
```

Related Commands

Command	Description
snmp-server host	Specifies the SNMP host to send the SNMP trap message.

Platform Description N/A

4.11 snmp-server flow-control

Use this command to configure the SNMP flow control. Use the **no** form of this command to restore the default setting.

snmp-server flow-control pps [*count*]

no snmp-server flow-control pps

Parameter Description

Parameter	Description
count	Indicates the number of SNMP requests processed per second, ranging from 50 to 65,535.

Defaults The default count is 300.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the number of SNMP requests processed per second to 200.

```
FS(config)# snmp-server flow-control pps 200
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.12 snmp-server group

Use this command to configure a new SNMP group**.** Use the **no** form of this command to remove a specified SNMP group.

snmp-server group *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { [*aclnum* | *aclname* }]

no snmp-server group *groupname* {**v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }

Parameter Description

Parameter	**Description**
v1 | **v2c** | **v3**	Specifies the SNMP version
auth	Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only.
noauth	Specifies no authentication a packet. This applies to SNMPv3 only.
priv	Specifies authentication of a packet with encryption. This applies to SNMPv3 only.
readview	Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent.
writeview	Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
aclnum	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.

Defaults No SNMP groups are configured by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures a new SNMP group.

```
FS(config)# snmp-server group mib2user v3 priv read mib2
```

Related Commands

Command	**Description**
show snmp group	Displays the SNMP group configuration.

Platform Description N/A

4.13 snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message. Use the **no** form of this command to remove the specified SNMP host.

snmp-server host [**oob**] { *host-addr* } [**traps | informs**] [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**]] *community-string* [**udp-port** *port-num*] [*notification-type*]

no snmp-server host [**oob**] { *host-addr* } [**traps | informs**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*]

Parameter Description

Parameter	Description
oob	Indicates the out of band communication, that is, the trap messages are sent to the alarm server through the MGMT port. This option is available only when the device is equipped with the MGMT port.
host-addr	SNMP host address
trap | informs	Enables the host to send the SNMP notification as traps or informs.
version	SNMP version: V1, V2C or V3
auth | **noauth** | **priv**	Security level of SNMPv3 users
community-string	Community string or username (SNMPv3 version)
port-num	Port of the SNMP host
notification-type	The type of the SNMP trap message, such as **snmp**. If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included.

Defaults No SNMP host is specified by default.

Command mode Global configuration mode.

Usage Guide This command must be used together with the **snmp-server enable traps** command to send the SNMP trap messages to NMS.

Multiple SNMP hosts can be configured to receive the SNMP trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations.

Configuration Examples The following example specifies an SNMP host to receive the SNMP event trap:

```
FS(config)# snmp-server host 192.168.12.219 public snmp
```

Related Commands

Command	Description
snmp-server enable traps	Enables the SNMP agent to send the SNMP trap message.

Platform Description N/A

4.14 snmp-server inform

Use this command to configure the resend times for inform requests and the inform request timeout**.** Use the **no** form of this command to restore the default settings.

snmp-server inform [**retries** *retry-time* | **timeout** *time*]

no snmp-server inform

Parameter Description

Parameter	Description
retry-num	Specifies the resend times for inform requests, ranging from 0 to 255.
time	Specifies the inform request timeout, ranging from 0 to 21,474,836.

Defaults The default *retry-num* is 3, and the default **timeout** *time* is 15 seconds.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the resend times of inform requests to 5.

```
FS(config)# snmp-server inform retries 5
```

The following example configures the inform request timeout to 20 seconds.

```
FS(config)# snmp-server inform timeout 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.15 snmp-server location

Use this command to set the system location string. Use the **no** form of this command to remove the system location string.

snmp-server location *text*

no snmp-server location

Parameter Description

Parameter	Description
text	String that describes the system location information.

Defaults No system location string is set by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples

The following example sets the system location information:

```
FS(config)# snmp-server location start-technology-city 4F of A Buliding
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact information.

Platform Description N/A

4.16 snmp-server net-id

Use this command to configure the network element coding information of the device. Use the **no** form of this command to remove the network element coding information.

snmp-server net-id *text*

no snmp-server net-id

Parameter Description

Parameter	Description
text	Configures the network element coding information of the device. The text length ranges from 1 to 255. The text is case-sensitive, and may contain spaces.

Defaults No network element coding information is configured by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples

The following example configures the network element coding text to FZ_CDMA_MSC1.

```
FS(config)# snmp-server net-id FZ_CDMA_MSC1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.17 snmp-server packetsize

Use this command to specify the largest size of the SNMP packet. Use the **no** form of this command to restore the default value.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameter Description

Parameter	Description
byte-count	Packet size. The range is from 484 to 17,876 bytes

Defaults The default is 1,472 bytes.

Command mode Global configuration mode.

Usage Guide The following example specifies the largest size of SNMP packet as 1,492 bytes:

```
FS(config)# snmp-server packetsize 1492
```

Configuration Examples N/A

Related Commands

Command	Description
snmp-server queue-length	Specifies the length of the message queue for each SNMP trap host.

Platform Description N/A

4.18 snmp-server queue-length

Use this command to specify the length of the message queue for each SNMP trap host. Use the **no** form of this command to restore the default value.

snmp-server queue-length *length*

no snmp-server queue-length

Parameter Description

Parameter	Description
length	Queue length. The range is from 1 to 1000.

Defaults The default is 10.

Command mode Global configuration mode.

Usage Guide Use this command to adjust the length of message queue for each SNMP trap host for the purposes of controlling the speed of sending the SNMP trap messages.

Configuration Examples The following example specifies the length of message queue as 100.

```
FS(config)# snmp-server queue-length 100
```

Related Commands

Command	Description
snmp-server packetsize	Specifies the largest size of the SNMP packet.

Platform Description N/A

4.19 snmp-server system-shutdown

Use this command to enable the SNMP message reload function. Use the **no** form of this command to disable the SNMP message reload function.

snmp-server system-shutdown

no snmp-server system-shutdown

Parameter Description

Parameter	Description
N/A	N/A

Defaults The SNMP message reload function is disabled by default.

Command mode Global configuration mode.

Usage Guide Use this command to enable the SNMP message reload function which may enable the system to send the device reload traps to the NMS before the device is reloaded or rebooted.

Configuration Examples The following example enables the SNMP message reload function:

```
FS(config)# snmp-server system-shutdown
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.20 snmp-server trap-format private

Use this command to configure the SNMP traps with private fields. Use the **no** form of this command to restore the default trap format.

snmp-server trap-format private

no snmp-server trap-format private

Parameter Description

Parameter	Description
N/A	N/A

Defaults The private field is not carried in the SNMP trap by default.

Command mode Global configuration mode.

Usage Guide Use this command to configure the SNMP trap format with the private field. Currently, the supported data in the private field is alarm occurrence time. For the specific data type and range of each field, refer to FS-TRAP-FORMAT-MIB.mib file.

This command does not work if the traps are sent with SNMPv1.

Configuration Examples The following example configures the SNMP trap format with the private field.

```
FS(config)# snmp-server trap-format private
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.21 snmp-server trap-source

Use this command to specify the source interface of the SNMP trap message. Use the **no** form of this command to restore the default value.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameter Description

Parameter	Description
interface	Specifies the source interface of the SNMP trap messages.

Defaults By default, the IP address of the interface from which the SNMP packet is sent is just the source address.

Command mode

Global configuration mode.

Usage Guide

For easy management and identification, you can use this command to fix a local IP address as the SNMP source address.

Configuration Examples

The following example specifies the IP address of Ethernet interface 0/1 as the source address of the SNMP trap message:

```
FS(config)# snmp-server trap-source fastethernet 0/1
```

Related Commands

Command	Description
snmp-server enable traps	Enables t the SNMP agent to send the SNMP trap massage to NMS.
snmp-server host	Specifies the NMS host to send the SNMP trap message.

Platform Description

N/A

4.22 snmp-server trap-timeout

Use this command to define the retransmission timeout time of the SNMP trap message. Use the **no** form of this command to restore the default value.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameter Description

Parameter	Description
seconds	Timeout (in seconds) of retransmit the SNMP trap message. The range is from 1 to 1,000.

Defaults

The default is 30 seconds.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example specifies the timeout period as 60 seconds.

```
FS(config)# snmp-server trap-timeout 60
```

Related

Command	Description

Commands

snmp-server queue-length	Specifies the length of message queue for the SNMP trap host.
snmp-server host	Specifies the NMS host to send the SNMP trap message.
snmp-server trap-source	Specifies the source address of the SNMP trap message.

Platform Description

N/A

4.23 snmp-server udp-port

Use this command to specify a port to receive SNMP packets**.** Use the **no** form of this command to restore the default setting.

snmp-server udp port *port-number*

no snmp-server udp port

Parameter Description

Parameter	**Description**
port-number	Specifies a port to receive the SNMP packets.

Defaults

The default is 161.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example specifies port 15000 to receive the SNMP packets.

```
FS(config)# snmp-server udp-port 15000
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

4.24 snmp-server user

Use this command to configure a new user to an SNMP group**.** Use the **no** form of this command to remove a user from an SNMP group.

snmp-server user *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { [*aclnum* | *aclname* }]]

no snmp-server user *username groupname* { **v1** | **v2c** | **v3** }

Parameter Description

Parameter	Description
username	Name of the user on the host that connects to the agent.
groupname	Name of the group to which the user belongs.
v1 | v2c | v3	Specifies the SNMP version. But only SNMPv3 supports the following security parameters.
encrypted	Specifies whether the password appears in cipher text. In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has a length of 16 bytes, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can be used only by the local SNMP engine on the switch.
auth	Specifies which authentication level should be used.
auth-password	Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.
priv	Encryption mode. des56 refers to 56-bit DES encryption protocol. *priv-password*: password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.
md5	Enables the MD5 authentication protocol. While the **sha** enables the SHA authentication protocol.
aclnumber	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
aclname	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.

Defaults N/A

Command mode Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

```
FS(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr
```

Related Commands

Command	Description
show snmp user	Displays the SNMP user configuration.

Platform Description

N/A

4.25 snmp-server view

Use this command to configure an SNMP view**.** Use the **no** form of this command to remove an SNMP view.

snmp-server view *view-name oid-tree* { **include** | **exclude** }

no snmp-server view *view-name* [*oid-tree*]

Parameter Description

Parameter	Description
view-name	View name
oid-tree	Specifies the MIB object to associate with the view.
include	Includes the sub trees of the MIB object in the view.
exclude	Excludes the sub trees of the MIB object from the view.

Defaults

By default, a view is set to access all MIB objects.

Command mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).

```
FS(config)# snmp-server view mib2 1.3.6.1 include
```

Related Commands

Command	Description
show snmp view	Displays the SNMP view configuration.

Platform Description

N/A

5 CM-APM Commands

5.1 apm conference-system access-list

Use this command to specify data flows that need video conference quality monitoring according to an ACL.

apm conference-system access-list *acl_id* **alias** *name*

Use the **no** form of this command to delete an ACL.

no apm conference-system access-list *acl_id*

Use the **no** form of this command to delete all ACLs.

no apm conference-system access-list all

Parameter Description

Parameter	Description
acl_id	Indicates the ID of an ACL. The value range is 1 to 199.
name	Indicates an alias of a data flow that matches a rule.

Defaults No data flow is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to specify data flows that need video conference quality monitoring.

Configuration Example

1. #Monitor all UDP flows transmitted between 172.18.3.3 and 172.18.3.8.

```
FS(config)# access-list 150 permit udp 172.18.3.3 0.0.0.0 172.18.3.8 0.0.0
FS(config)# apm conference-system access-list 150 alias kkk
```

2. #Delete the foregoing ACL.

```
FS(config)#no apm conference-system access-list 150
```

3. #Cancel all ACLs.

```
FS(config)# no apm conference-system access-list all
```

Verification Run the **show run | include apm conference-system access-list** command to display the ACLs that are monitored.

5.2 apm conference-system application

Use this command to specify applications that need video conference quality monitoring according to application names.

apm conference-system application *app_name*

Use the **no** form of this command to delete configurations of an application.

no apm conference-system application *app_name*

Use the **no** form of this command to delete configurations of all applications.

no apm conference-system application all

Parameter Description

Parameter	Description
app_name	Indicates an application name. This parameter cannot be set to **all**.

Defaults No application is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to specify applications that need video conference quality monitoring.

Configuration Example

#Specify the InfowareLab conference system to be monitored.

```
FS(config)# apm conference-system application InfowareLab conference system
```

#Cancel the monitoring on the InfowareLab conference system.

```
FS(config)#no apm conference-system application InfowareLab conference system
```

#Cancel the monitoring on all applications.

```
FS(config)# no apm conference-system application all
```

Verification Run the **show run | include apm conference-system application** command to display the applications that are monitored.

5.3 apm conference-system enable

Use this command to enable the video conference quality monitoring function.

apm conference-system enable

Use the **no** form of this command to disable the video conference quality monitoring function.

no apm conference-system enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The video conference quality monitoring function is enabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the video conference quality monitoring function. Use the no form of this command to disable the video conference quality monitoring function without deleting the application or access list.

Configuration Example

#Enable the video conference quality monitoring function.

```
FS(config)# apm conference-system enable
```

#Disable the video conference quality monitoring function.

```
FS(config)# no apm conference-system enable
```

Verification

Run the **show run** command to display this command. If this command is not available, the function is enabled.

5.4 apm conference-system measure-period

Use this command to configure the video conference monitoring period.

apm conference-system measure-period *time*

Use the **no** form of this command to delete the setting of the video conference monitoring period.

no apm conference-system measure-period

Parameter Description

Parameter	Description
time	Indicates the monitoring period in seconds. The value range is 30 to 120.

Defaults

The monitoring period is 60 seconds by default.

Command Mode

Configuration mode

Usage Guide

Use this command to configure the video conference monitoring period.

Configuration Example

#Set the monitoring period to 30 seconds.

```
FS(config)# apm conference-system measure-period 30
```

#Restore the default monitoring period.

```
FS(config)#no apm conference-system measure-period
```

Verification

N/A

5.5 apm export-length

Use this command to set the maximum length of valid packet data of APM logs.

apm export-length *value*

Use the **no** form of this command to restore the default configuration.

no apm export-length

Parameter Description

Parameter	Description
value	Indicates the length of valid data in ipfix packets. The length is measured from the TCP or UDP valid data in bytes. The value range is 300 to 1,400.

Defaults The maximum length of valid data is 1,400 bytes by default.

Command Mode Global configuration mode

Usage Guide The default value is 1400. Generally, the default value is used by default and does not need to be configured. If the parameter is set to a larger value, bandwidth consumption is reduced.

Configuration Example #Set the maximum length of valid packet data of APM logs to 1,000 bytes.

```
FS(config)#apm export-length 1000
```

#Restore the default length of ipfix packets.

```
FS(config)#no apm export-length
```

Verification Run the **show apm server info** command to display the configuration result.

5.6 apm export-rate

Use this command to set the APM log transmission rate.

apm export-rate *rate*

Use the **no** form of this command to restore the default configuration.

no apm export-rate

Parameter Description

Parameter	Description
rate	Indicates the number of APM logs that are sent per second. The value range is 10 to 100,000.

Defaults The transmission rate is 1,000 logs per second by default.

Command Mode Global configuration mode

Usage Guide The default transmission rate is 1,000 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.

Configuration Example #Set the transmission rate to 100 ipfix nodes (not packets) per second.

```
FS(config)# apm export-rate 100
```

#Restore the default configuration.

```
FS(config)# no apm export-rate
```

Verification Run the **show apm server info** command to display the configuration result.

5.7 apm log-type

Use this command to specify a server to receive APM logs.

apm log-type {*type* | **default**} **priority** *prio* **server** *name*

Use the **no** form of this command to delete the configuration.

no apm log-type { type **| default | all }**

Parameter Description

Parameter	Description
type	Indicates an APM log type. Run the **show apm log-type** command to display the log type indicated by each value.
prio	Indicates a priority of a log type. The value range is 0 to 2. The value 0 indicates the highest priority.
name	Indicates a name of a server that receives APM logs.

Defaults No server for receiving AMP logs is configured by default.

Usage Guide Use this command to specify priorities of log types and the APM log server to receive the logs. A log can be sent to one server only. The parameter **default** indicates that 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 the default log type, 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.

Configuration Example

#Use the default server RAC to receive all types of logs. The priority is 0.

```
FS(config)# apm log-type default priority 0 server rac
```

#Delete the default log type configuration.

```
FS(config)# no apm log-type default
```

#Delete the server configuration of all log types.

```
FS(config)# no apm log-type all
```

#Set logs of log-type 1 to be sent to the server FS, and priority to 1.

```
FS(config)#apm    log-type 1 priority 1 server FS
```

#Delete the special configuration of log-type 1.

```
FS(config)# no apm log-type 1
```

Verification Run the **show apm server info** command to display the server and priority configuration.

5.8 apm sample business application

Use this command to configure services to be monitored

apm sample business application *app-name*

Use the **no** form of this command to cancel the monitoring on a service.

no apm sample business application *app-name*

Use the **no** form of this command to cancel the monitoring on all services.

no apm sample business application all

Parameter Description

Parameter	Description
app-name	Indicates an application name. For details, refer to the APP-IDENTITY configuration guide.

Defaults No service is configured by default.

Usage Guide Use this command to specify a service (application) to be monitored, which relies on the accuracy of the application identification result. At present, no more than 50 applications can be specified.

Configuration Example

#Monitor the BQQ data throughput.

```
FS(config)# apm sample business application BQQ
```

#Cancel the monitoring on the BQQ data throughput.

```
FS(config)# no apm sample business application BQQ
```

#Cancel the monitoring on all services.

```
FS(config)# no apm sample business application all
```

Verification Run the **FS#show apm sample business info** command to display the configuration result.

5.9 apm sample disable

Use this command to disable specified APM monitoring functions.

apm sample { cpu-mem | sata-flash | vpn | vpn-detail | ip-session | intf-flowrate | app-type-flowrate | app-flowrate | user-flowrate | ping-detect | url-topn | business } disable

Use the **no** form of this command to enable specified APM monitoring functions.

no apm sample{ cpu-mem | sata-flash | vpn | vpn-detail | ip-session | intf-flowrate | app-type-flowrate | app-flowrate | user-flowrate | ping-detect | url-topn | business } disable

Use this command to enable all APM monitoring functions.

apm sample del-all-disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

All APM monitoring functions are enabled by default.

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).

cpu-mem: Indicates the CPU and memory usage.

sata-flash: Indicates the hard disk and flash memory usage.

vpn: Indicates the VPN status (connected or disconnected).

vpn-detail: Indicates 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.

Configuration Example

#Disable CPU and memory monitoring.

```
FS(config)# apm sample cpu-mem disable
```

#Disable application traffic monitoring.

```
FS(config)# apm sample app-flowrate disable
```

#Enable application traffic monitoring.

```
FS(config)# no apm sample app-flowrate disable
```

Verification

Run the **FS#show running-config | include apm sample** command to display the statuses of the functions.

5.10 apm sample enable

Use this command to enable global APM monitoring.

apm sample enable

Use the **no** form of this command to disable global APM monitoring.

no apm sample enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Global APM monitoring is disabled by default.

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.

Configuration Example #Enable global APM monitoring.

```
FS(config)# apm sample enable
```

#Disable global APM monitoring.

```
FS(config)# no apm sample enable
```

Verification Run the **show running-config | include apm sample** command to display the status of the function.

5.11 apm sample interval

Use this command to configure the global APM monitoring period.

apm sample default interval *second*

Use the **no** form of this command to restore the default global monitoring period.

no apm sample default interval

Use this command to configure the monitoring periods of different monitoring functions.

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*

Use the **no** form of this command to restore the default monitoring periods of specified APM monitoring functions.

no apm sample { cpu-mem | sata-flash | vpn | vpn-detail | ip-session | intf-flowrate | app-type-flowrate | app-flowrate | user-flowrate | ping-detect | business } interval

Parameter Description

Parameter	Description
second	Indicates the monitoring period in seconds. The value range is 10 to 3,600.

Defaults The global APM monitoring period is five minutes by default. Monitoring period is not set for a single APM monitoring function by default.

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.

Configuration Example

#Set the monitoring period of the CPU and memory to 10 seconds.

```
FS(config)# apm sample cpu-mem interval 10
```

#Set the monitoring period of the application traffic to 10 seconds.

```
FS(config)# apm sample app-flowrate interval 10
```

#Restore the default monitoring period of the application traffic.

```
FS(config)# no apm sample app-flowrate interval
```

Verification

Run the **show apm sample log-sends** command to display the configuration result.

5.12 apm sample ping-detect server

Use this command to configure a server to be pinged.

apm sample ping-detect server { *ip-address* | *host* } **[ntimes** *times***] [length** *len***] [source {lan** | *so-ip-address* | *interface-name* } **]**

Use the **no** form of this command to delete a specified pinged server.

no apm sample ping-detect server { *ip-address* | *host* }

Use the **no** form of this command to delete all pinged servers.

no apm sample ping-detect server all

Parameter Description

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 range is 1 to 10.
len	Indicates the length of a ping packet. The value range is 64 to 1,400.
so-ip-address	Indicates the source IP address in a ping packet.
interface-name	Indicates the name of an interface.

Defaults

Five packets are sent for each ping test, and the length of a ping packet is 100 by default.

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 is optional.

Configuration Example

#Set the IP address of a server to be pinged to 172.18.3.1, number of ping packets to 10, and packet length to 100 bytes.

```
FS(config)# apm sample ping-detect server 172.18.3.1 ntimes 10 length 100
```

#Delete the pinged server at 172.18.3.1.

```
FS(config)# no apm sample ping-detect server 172.18.3.1
```

#Delete all pinged servers.

```
FS(config)# no apm sample ping-detect server all
```

Verification

Run the **show apm sample ping-detect info** command to display the configuration result.

5.13 apm sample url-topn send-time

Use this command to configure URL-TOPN transmission time.

apm sample url-topn send-time *hour*

Use the **no** form of this command to restore the default configuration.

no apm sample url-topn send-time

Parameter Description

Parameter	Description
hour	Specifies the URL-TOPN transmission time. The value range is 0 to 23.

Defaults

URL-TOPN transmission time is 01:00 by default.

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.

Configuration Example

#Set the URL-TOPN transmission time to 00:00.

```
FS(config)# apm sample url-topn send-time 0
```

#Restore the default configuration.

```
FS(config)# no apm sample url-topn send-time
```

Verification

Run the **show apm sample url-topn info** command to display the configuration result.

5.14 apm sample url-topn top

Use this command to configure a behavior report URL-TOPN.

apm sample url-topn top *num*

Use the **no** form of this command to restore the default configuration.

no apm sample url-topn top

Parameter Description

Parameter	Description
num	Specifies the number of top URLs to be collected. The value range is 1 to 100.

Defaults

The top 50 URLs are sent by default.

Usage Guide

Use this command to set the number of top URLs to be sent.

Configuration Example

#Set top 80 URLs to be sent.

```
FS(config)# apm sample url-topn top 80
```

#Restore the default configuration.

```
FS(config)# no apm sample url-topn top
```

Verification

Run the **show apm sample url-topn info** command to display the configuration result.

5.15 apm server

Use this command to set an APM log server.

apm server *name* { *ip-address* } [**source** *sip-address*] [*port*] **[tcp | udp] [oob]**

Use the **no** form of this command to delete a specified log server.

no apm server *name*

Use the **no** form of this command to delete all log servers.

no apm server all

Parameter Description

Parameter	Description
name	Indicates the name of an APM log server.
ip-address	Indicates the IP address of the APM log server.
sip-address	Indicates the local source IP address that is bound to the APM log server.
port	Indicates the port number of the APM log server.

Defaults

The port of the APM log server is 30000, and the protocol is TCP by default.

Usage Guide

Use this command to specify the TCP or UDP protocol for APM log transmission. TCP is the default and recommended protocol. No more than 10 servers can be configured.

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.

Configuration Example

#Configure the RAC server as a log server, and set the port to 20000 and protocol to UDP.

```
FS(config)# apm server rac 172.18.3.51 20000 udp
```

#Configure the RAC server as a log server, and set the source IP address to 192.168.1.1.

```
FS(config)# apm server rac 172.18.3.51 source 192.168.1.1
```

#Change the IP address of the RAC server.

```
FS(config)# apm server rac 172.18.3.52
```

#Delete the source IP address, that is, unbound the server from the source IP address.

```
FS(config)# apm server rac 172.18.3.52 source 0.0.0.0
```

#Delete the RAC server.

```
FS(config)# no apm server rac
```

#Delete all log servers.

```
FS(config)# no apm server all
```

Verification

1. Run the **show apm server info** command to display the configuration result. The value of **socket** is not 0.
2. Check whether the configured server receives logs.

5.16 apm template send-period

Use this command to configure the APM template transmission period.

apm template send-period *seconds*

Use the **no** form of this command to restore the default configuration.

no apm template send-period

Parameter Description

Parameter	Description
seconds	Indicates the template transmission period (in seconds). The value range is 60 to 3,600.

Defaults The APM template transmission period is 300 seconds by default.

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

#Set the APM template transmission period to 60 seconds.

```
FS(config)# apm template send-period 60
```

#Restore the default configuration.

```
FS(config)# no apm template send-period
```

Verification

1. Run the **show apm server info** command to display the configuration result.
2. Configure a server which is not associated with any log type, and then run the **clear apm server log-count** command to clear the count. After a period of time, check for data output, and measure the time difference between two consecutive counts to check whether the period is the configured time.

5.17 apm user-log filter

Use this command to configure fields to filter audit logs.

apm user-log filter *words*

Use the **no** form of this command to cancel the fields that are used to filter audit logs.

no apm user-log filter *words*

Parameter Description

Parameter	Description
words	Indicates the fields that are used to filter logs.

Defaults

N/A

Command Mode

Configuration mode

Usage Guide

Use this command to specify keywords, so as to filter audit logs that are not required.

Configuration Example

#Configure the word **login** as a condition to filter audit logs.

```
FS(config)# apm user-log filter login
```

#Cancel the filtering configuration.

```
FS(config)# no apm user-log filter login
```

Verification

Run the **show apm user-log filter** command to display the configuration result.

5.18 apm webpage enable

Use this command to enable webpage loading time measurement.

apm webpage enable

Use the **no** form of this command to disable webpage loading time measurement.

no apm webpage enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Webpage loading time measurement is enabled by default.

Command Mode Configuration mode

Usage Guide This function is enabled by default. If no webpage is configured, performance is not affected.

If multiple webpages are configured, use the no form of this command to disable the function.

Configuration Example #Enable webpage loading time measurement.

```
FS(config)# apm webpage enable
```

#Disable webpage loading time measurement.

```
FS(config)# no apm webpage enable
```

Verification Run the **show apm webpage statistics** command to display the status of this function.

5.19 apm webpage url

Use this command to configure URLs to be monitored.

apm webpage url *url-string*

Use the **no** form of this command to cancel the monitoring on the URLs.

no apm webpage url [**all** | *url-string*]

Parameter Description

Parameter	Description
url-string	Indicates the URLs to be monitored.

Defaults -

Command Mode Global configuration mode

Usage Guide Use this command to configure a URL to be monitored.

Use the **no** form of this command to cancel the monitoring on a URL.

Use the **no apm webpage url** all command to cancel monitoring on all URLs.

The URLs are precisely matched.

Configuration #Configure www.ietf.com as a URL to be monitored.

Example

```
FS(config)# apm webpage url www.ietf.com/
```

#Cancel the monitoring on the URL.

```
FS(config)# no apm webpage url www.ietf.com/
```

#Cancel the monitoring on all URLs.

```
FS(config)# no apm webpage url all
```

Verification Run the **show apm webpage url** command to display the URLs being monitored.

5.20 clear apm server log-count

Use this command to clear transmission statistics about APM logs.

clear apm server log-count

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear transmission statistics about APM logs. The count should be 0.

Configuration Example

#Clear transmission statistics about APM logs.

```
FS#clear apm server log-count
```

5.21 show apm sample business info

Use this command to display services (applications) to be monitored.

show apm sample business info

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display services (applications) to be monitored.

Configuration Example

#Display services (applications) to be monitored.

```
FS#show apm sample business info
Other TCP
BQQ
QQ-login|chat
```

```
MAPI
DNS
telnet
NETBIOS-NS
```

Field description:

Field	Description
	Displays the name of a service being monitored.

5.22 show apm sample log-sends

Use this command to display monitoring periods of different services.

show apm sample log-sends

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display monitoring periods of different services.

Configuration Example #Display monitoring periods of different services.

```
FS#show apm sample log-sends
log-name                    interval
cpu-mem                        10
sata-flash                  10
ip-session                  10
intf-flowrate              10
app-type-flowrate           10
app-flowrate                 10
user-flowrate               10
vpn                           10
vpn-detail                  10
business                     10
ping-detect                  10
url-topn                     300
```

Field description:

Field	Description
log-name	Indicates the name of a log type.
interval	Indicates the log transmission period in seconds.

5.23 show apm sample ping-detect info

Use this command to display user-defined ping test information.

show apm sample ping-detect info

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display user-defined ping test information.

Configuration Example

#Display user-defined ping test information.

```
FS#show apm sample ping-detect info
--------------------------------------------------------------
server1:172.18.3.1
ntimes:10          length:1400          source:
--------------------------------------------------------------
server2:172.18.3.100
ntimes:10          length:1400          source:
```

Field description

Field	Description
server	Indicates the IP address or URL of a server.
ntimes	Indicates the number of ping packets.
length	Indicates the length of a ping packet.
source	Indicates the source IP address in a ping packet. If this parameter is null, the default setting of the gateway is used.

5.24 show apm sample url-topn info

Use this command to display user-defined URL-TOPN information.

show apm sample url-topn info

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display user-defined URL-TOPN information.

Configuration Example

#Display user-defined URL-TOPN information.

```
FS#show apm sample url-topn info
send-clock: 1
send-topn: 50
```

Field description:

Field	Description
send-clock	Indicates the log transmission time.
send-topn	Indicates the number of top N URLs to be sent.

5.25 show apm server info

Use this command to display APM log server configuration.

show apm server info

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display APM log server configuration.

Configuration Example #Display APM log server configuration.

```
FS#show apm server info
Ipfix server is enable!
========================================================================
server:server1                    ip:172.18.181.63     port:30000 protocal:udp
socket : 32857
========================================================================
server:server2                    ip:172.18.3.56       port:20000 protocal:tcp
socket : 0
log_type:1      prio:0
========================================================================
server:server3               ip:172.18.181.63     port:20000 protocal:udp
socket : 32858
========================================================================
Export rate : 1000
Template send period second : 300
Send buffer length : 1400
ipfix queue free node number : 3000
ipfix msg queue node info
prio : 0, msg node number : 0
prio : 1, msg node number : 0
prio : 2, msg node number : 0
Create template error number: 0
Record data error number: 25060
```

Field description:

Field	Description
The first line of the show result	Indicates the availability of a server.

server	Indicates the server name.
ip	Indicates the IP address of a server.
port	Indicates the server port.
protocal	Indicates a protocol used for transmitting packets.
socket	Specifies a socket value. The value 0 indicates that the server is unavailable. A non-zero value indicates the socket value.
log_type	Mounts a log type to a corresponding server.
prio	Indicates the priority of a log type.
Export rate	Indicates the number of the nodes sent per second.
Template send period second	Indicates the packet transmission period.
Send buffer length	Indicates the maximum length of an ipfix packet.
ipfix queue free node number	Indicates the number of ipfix idle nodes.
ipfix msg queue node info	Indicates the number of nodes corresponding to each priority.
Create template error number	Indicates the number of template creation failures.
Record data error number	Indicates the number of data writing failures. Run the **clear apm server log-count** command to clear the count.

5.26 show apm server log-count

Use this command to display the number of transmitted APM logs.

show apm server log-count

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the number of transmitted APM logs.

Configuration Example

```
FS#show apm server log-count
Server : server1
Send node num: 10 send packet : 24692 error packet : 380
last_error:server socket closed (51)
Drop node num : 0
=====================================================================
Server : server2
Send node num: 0 send packet : 0 error packet : 0 last_errno : 0
last_error:......
Drop node num : 200576
=====================================================================
Server : server3
Send node num: 10 send packet : 24692 error packet : 380 last_errno: 51
last_error:......
Drop node num : 0
=====================================================================
<1>cpu-memory                   , send log num: 1
<2>flash-sata                  , send log num: 2
<3>ip-session                   , send log num: 3
<4>intf-flowrate               , send log num: 4
<5>app-type-flowrate       , send log num: 5
<6>app-flowrate                , send log num: 6
<7>user-flowrate              , send log num: 7
<8>vpn-infomation             , send log num: 8
<9>vpn-detail                   , send log num: 9
<10>webpage-time              , send log num: 0
<11>conference-system      , send log num: 10
<12>config-infomation      , send log num: 10
<13>business-flowrate      , send log num: 10
<14>ping-detect                , send log num: 10
<15>url-top-n                   , send log num: 10
<16>tcp-performance         , send log num: 10
<17>udp-performance         , send log num: 10
```

Field description:

Field	Description
Server	Indicates the server name.
Send node num	Indicates the number of the sent nodes.
send packet	Indicates that multiple packets are sent to the server.
error packet	Indicates the number of sent error packets.
last_error	Indicates the cause for the last transmission failure. The information in brackets indicates the error code.
Drop node num	Indicates the number of nodes of which queues are full and cannot be joined in.
send log num	Indicates the number of sent logs of a type.

5.27 show apm tcp-measure info

Use this command to display the TCP measurement information.

show apm tcp-measure info

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide

Use this command to display TCP performance measurement information, including the number of flows being measured, number of duplicate packets, and number of output logs.

Configuration Example

#Display the TCP measurement information.

```
FS#show apm tcp-measure info
Flow capacity: 2000, used num:0
Duplicate capacity: 8000, used num:0
Send Logs: 988
```

Field description:

Field	Description
Flow capacity	Indicates the nodes that are used to measure flows, including the maximum number of nodes and number of used nodes.
Duplicate capacity	Indicates the nodes used to measure duplicate packets, including the maximum number of nodes and number of used nodes.
Send Logs	Indicates the number of sent logs.

5.28 show apm udp-measure info

Use this command to display UDP flow information of a video conference being monitored.

show apm udp-measure info

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display UDP flow information of a video conference being monitored.

Configuration Example

#Display UDP flow information of a video conference being monitored.

```
FS# show apm udp-measure info
the udp monitor buffer is : 5112
the udp monitor bank: 248
the sector head num    :111
dst_ip              src_ip            dst _port     src_port        direct      packet_code
172.18.3.8          172.18.3.3        8000           1863             2            24e551a1
172.18.3.3          172.18.3.8        1863           8000             1            e61d5c16
```

Field description:

Field	Description

udp monitor buffer	Indicates the number of idle buffers assembled.
udp monitor bank	Indicates the number of idle windows.
sector head	Indicates the number of idle 5-tuples monitored.
dst_ip	Indicates a destination IP address.
src_ip	Indicates a source IP address.
dst_port	Indicates a destination port.
src_port	Indicates a source port.
direct	Indicates the packet direction. The value 1 indicates the downlink direction, and the value 2 indicates the uplink direction.
packet_code	Indicates the code of the first packet.

5.29 show apm webpage statistics

Use this command to display running information measured during webpage loading.

show apm webpage statistics

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display running information measured during webpage loading, including the number of webpages, number of connections, number of sent logs, and module running status.

Configuration Example

#Display running information measured during webpage loading.

```
FS#show apm webpage statistics
apm webpage info:
    export log num:0
    webpage capacity: 1000; used:        0
    connection capacity: 2000; used:        0
webpage : disable
```

Field description:

Field	Description
export log num	Indicates the number of sent logs about the webpage loading time.
webpage capacity	Indicates the maximum number of nodes and number of used nodes.
connection capacity	Indicates the maximum number of webpage connections and number of used webpage connections.
webpage	Indicates the module running status (processing packets).

5.30 show apm webpage url

Use this command to display webpage URLs being monitored.

show apm webpage url

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display details about the webpage URLs being monitored.

Configuration Example

#Display details about the webpage URLs being monitored.

```
FS#show apm webpage url
www.ietf.com/
www.ietf.com/index.html
```

Field description:

Field	Description
www.ietf.com/	Indicates a webpage URL.

6 ANTI-SNIPER Commands

6.1 anti-sniper interface

Use this command to enable anti-sniper.

anti-sniper interface *intf-name*

Use the **no** form of this command to disable anti-sniper..

no anti-sniper interface *intf-name*

Parameter Description

Parameter	Description
intf-name	Specifies an interface.

Defaults Anti-sniper is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Example

#Enable anti-sniper on interface GI0/5

```
FS#config
FS(config)#anti-sniper interface gigabitEthernet 0/5
```

#Disable anti-sniper on interface GI0/5

```
FS#config
FS(config)# no anti-sniper interface gigabitEthernet 0/5
```

6.2 http-modify off

Use this command to enable HTTP packet splitting.

http-modify off

Use the **no** form of this command to disable HTTP packet splitting.

no http-modify off

Parameter Description

Parameter	Description
N/A	N/A

Defaults HTTP packet splitting is enabled by default.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example

#Enable HTTP packet splitting.

```
FS#config
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
```

6.3 http-modify mode

Use this command to configure the HTTP packet splitting mode.

http-modify mode *num*

Use the **no** form of this command to remove the configuration..

no http-modify mode

Parameter Description

Parameter	Description
num	Specifies the HTTP packet splitting mode, in the range from 1 to 4.

Defaults The default value is 1.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example

#Set the HTTP packet splitting mode to 3.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# anti-sniper interface gigabitEthernet 0/5
FS(config-anti-sniper)# http-modify mode 3
```

6.4 ip-id off

Use this command to disable packet IPID modification.

ip-id off

Use the **no** form of this command to enable packet IPID modification.

no ip-id off

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example #Enable packet IPID modification.

```
FS#config
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
```

6.5 ip-id random

Use this command to set the packet IPID to a random value.

ip-id random

Use the **no** form of this command to set the packet IPID to an ascending value.

no ip-id random

Parameter Description

Parameter	Description
N/A	N/A

Defaults The packet IPID is a random value by default.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example #Set packet IPID to a random value.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# anti-sniper interface gigabitEthernet 0/5
FS(config-anti-sniper)#ip-id random
```

6.6 ip-ttl off

Use this command to disable packet TTL modification.

ip-ttl off

Use the **no** form of this command to enable packet TTL modification.

no ip-ttl off

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example #Disable packet TTL modification.

```
FS#config
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
```

6.7 ip-ttl value

Use this command to set the TTL value.

ip-ttl value *num*

Use the **no** form of this command to remove the configuration.

no ip-ttl value

Parameter Description

Parameter	Description
num	Specifies a TTL value, in the range from 1 to 255.

Defaults The default value is 128.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example #Set the TTL value to 127.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# anti-sniper interface gigabitEthernet 0/5
FS(config-anti-sniper)# ip-ttl value 127
```

6.8 tcp-port off

Use this command to disable TCP port modification.

tcp-port off

Use the **no** form of this command to enable TCP port modification.

no tcp-port off

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example

#Enable TCP port modification.

```
FS#config
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
```

6.9 tcp-port continuous

Use this command to set the TCP port number to a continuous value.

tcp-port continuous

Use the **no** form of this command to set the TCP port number to an odd-even interleaving value.

no tcp-port continuous

Parameter Description

Parameter	Description
N/A	N/A

Defaults The TCP port number is a continuous value by default.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example

#Set the TCP port number to a continuous value.

```
FS#config
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 continuous
```

6.10 tcp-port range

Use this command to set the TCP port range.

tcp-port range *min-port max-port*

Use the **no** form of this command to remove the configuration.

no tcp-port range

Parameter Description

Parameter	Description
min-port	Specifies the minimum port number, in the range from 1 to 65535. Default: 1054.
max-port	Specifies the maximum port number, in the range from 1 to 65535. Default: 9000.

Defaults

The default TCP port range is from 1054 to 9000.

Command Mode

Anti-sniper mode

Usage Guide

N/A

Configuration Example

#Set the TCP port range from 2000 to 8000.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# anti-sniper interface gigabitEthernet 0/5
FS(config-anti-sniper)# tcp-port range 2000 8000
```

6.11 tcp-timestamp off

Use this command to disable TCP timestamp.

tcp-timestamp off

Use the **no** form of this command to enable TCP timestamp.

no tcp-timestamp off

Parameter Description

Parameter	Description
N/A	N/A

Defaults

TCP timestamp is enabled by default.

Command Mode

Anti-sniper mode

Usage Guide

N/A

Configuration Example

#Enable TCP timestamp.

```
FS#config
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
```

6.12 tcp-win-size off

Use this command to disable TCP window size modification.

tcp-win-size off

Use the **no** form of this command to enable TCP window size modification.

no tcp-win-size off

Parameter Description

Parameter	Description
N/A	N/A

Defaults TCP window size modification is enabled by default.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example

#Enable TCP window size modification.

```
FS#config
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
```

6.13 tcp-win-size value

Use this command to set the TCP window size.

tcp-win-size value *num*

Use the **no** form of this command to remove the configuration.

no tcp-win-size value

Parameter Description

Parameter	Description
num	Sets the TCP window size, in the range from 1 to 65535.

Defaults The default TCP window size is 65535.

Command Mode Anti-sniper mode

Usage Guide N/A

Configuration Example

#Set the TCP window size to 65535.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# anti-sniper interface gigabitEthernet 0/5
FS(config-anti-sniper)# tcp-win-size value 65535
```

6.14 show anti-sniper policy

Use this command to display anti-sniper configuration.

show anti-sniper policy

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Example

#Display anti-sniper configuration.

```
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        : FALSE
tcp-port range               : 1054-9000
tcp-win-size                  : ON
tcp-win-size value         : 65535
tcp-timestamp                 : ON
http-modify                    : ON
http-modify mode            : 1
```

Chapter 9 Reliability Configuration Commands

1 VRRP Commands

1.1 show vrrp

Use this command to display the VRRP information.

show vrrp [**brief** | *group*]

Parameter Description

Parameter	Description
brief	(Optional) Displays the brief of the VRRP group.
group	Number of the VRRP group to be displayed

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

If no optional parameter is used, the information of all VRRP groups is displayed.

Configuration Examples

The following example displays the information of all VRRP groups.

```
FS# show vrrp
FastEthernet 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 Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 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 Device is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FS#
```

The following example displays the brief information of the VRRP group.

```
FS# show vrrp brief
Interface     Grp Pri timer    Own Pre State      Master addr        Group addr
Gi 0/0         1 100    10.82       -     P    Backup    192.168.201.213 192.168.201.1
Gi 0/0         2 120    10.59       -     P    Master    192.168.201.217 192.168.201.2
FS#show ipv6 vrrp brief
Interface           Grp Pri timer Own Pre State Master addr    Group addr
Gi0/13                    1 100 3.60 -    P    Master FE80::1                        FE80::2
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.

Platform Description

N/A

1.2 show vrrp interface

Use this command to display the information of the VRRP on the interface.

show vrrp interface *type number* [**brief**]

Parameter Description

Parameter	Description
type	Interface type
number	Interface number
brief	(Optional) Displays the brief of the VRRP group on the interface.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the VRRP information on Ethernet interface E1/0.

```
FS# show vrrp interface fastethernet 0/0
FastEthernet 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 Device is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 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 Device is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
```

Related Commands

Command	Description
vrrp *group* **ip** *ip address* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device

Platform Description

N/A

1.3 show vrrp packet statistics

Use this command to display the statistics of the VRRP packet transmission.

show vrrp packet statistics [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Interface type and number

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the statistics of VRRP packet transmission on all interfaces.

```
FS# show vrrp packet statistics

Total
    InReceives: 966043 packets, InOctets: 38641824, InErrors: 38826
    OutTransmits: 306079, OutOctets: 7798564
GigabitEthernet 3/0/1
    InReceives: 799665 packets, InOctets: 31986600, InErrors: 19657
    OutTransmits: 272931, OutOctets: 6675320
GigabitEthernet 3/0/2
    InReceives: 0 packets, InOctets: 0, InErrors: 0
    OutTransmits: 681, OutOctets: 16344
```

The following example displays the statistics of VRRP packets on the interface gigabitEthernet 3/0/1.

```
FS#show vrrp packet statistics gigabitEthernet 3/0/1
GigabitEthernet 3/0/1
    InReceives: 799911 packets, InOctets: 31996440, InErrors: 19657
    OutTransmits: 273053, OutOctets: 6677760
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.4 vrrp authentication

Use this command to enable VRRP authentication.

Use the **no** form of this command to disable this function.

vrrp *group* **authentication** *string*

no vrrp *group* **authentication**

Parameter Description

Parameter	Description
group	VRRP group number
string	String for the VRRP group authentication (within 8 bytes, plaintext password)

Defaults

This function is disabled by default. Even if the VRRP function is enabled, no authentication password is configured by default.

Command Mode

Interface configuration mode

Usage Guide

The devices in the same VRRP group must have the same authentication password configured. The plaintext authentication password cannot provide security. It aims only to prevent/prompt the incorrect VRRP configuration. This command is only applied to the VRRPv2 packets.

Configuration Examples

The following example sets the authentication password for VRRP group 1.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)# vrrp 1 authentication x30dn78k
```

Platform Description

N/A

1.5 vrrp delay

Use this command to set the reload latency of the VRRP group on the interface.

Use the **no** form of this command to restore the default setting.

vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }

no vrrp delay

Parameter Description

Parameter	Description
minimum *min-seconds*	When the interface is up, VRRP group shall be reloaded after at least min-seconds.
reload *reload-seconds*	The reload latency of the VRRP group. If the configured *min-seconds* is more than *reload-seconds*, the actual reload latency of the VRRP group will be min-seconds.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to set the reload latency of the VRRP group on the interface, when it is required that the VRRP group shall not be reloaded immediately after the system reloads or the interface is up. The reload latency range is 0 to 60 seconds.

Configuration Examples

The following example sets the VRRP reload latency on E0 to 10 seconds. When E0 is up, VRRP group 1 shall be reloaded in 10 seconds.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#vrrp delay minimum 10 reload 10
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.6 vrrp description

Use this command to specify a descriptor for the VRRP.

Use the **no** form of this command to restore the default setting.

vrrp *group* **description** *text*

no vrrp *group* **description**

Parameter Description

Parameter	Description
group	VRRP group number
text	VRRP group descriptor

Defaults

This function is disabled by default. Even if the VRRP function is enabled, no VRRP group descriptor is configured by default.

Command Mode

Interface configuration mode

Usage Guide

This command will set the descriptor for the VRRP group to facilitate the identification of the VRRP group.

Configuration Examples

The following example labels the VRRP group 1 on Ethernet interface E0 as Building A – Marketing and Administration.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)#vrrp 1 description “Building A -
Marketing and Administration”
```

Related Commands

Command	Description
vrrp *group* **ip** *ip-address* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device

Platform Description

N/A

1.7 vrrp ip

Use this command to enable VRRP on the interface and specify the related virtual IP address.

Use the **no** form of this command to restore the default setting.

vrrp *group* **ip** *ipaddress* [**secondary**]

no vrrp *group* **ip** *ipaddress* [**secondary**]

Parameter Description

Parameter	Description
group	VRRP group number of the virtual device

ipaddress	IP address of the virtual device
secondary	Specifies the secondary IP address of the virtual device.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

If the **secondary** parameter is not used, the IP address set here will become the master IP address of the virtual device. Note that if the VRRP group is using the IP address of the Ethernet interface, an error occurs when you remove the IP address of the VRRP group with the **no** command, because there are duplicated IP addresses in the LAN.

Configuration Examples

The following example enables the VRRP function on Ethernet interface 0. The VRRP group number is 1, primary IP address of the virtual device is 10.0.1.20 and secondary IP address is 10.0.2.20.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.2.1 255.255.255.0 secondary
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.2.20 secondary
```

Related Commands

Command	Description
show vrrp [**brief** | **group**]	Displays the VRRP configuration.

Platform Description

N/A

1.8 vrrp preempt

Use this command to set the preemption mode of the VRRP group.

Use the **no** form of this command to restore the default setting.

vrrp *group* **preempt** [**delay** *seconds*]

no vrrp *group* **preempt** [**delay**]

Parameter Description

Parameter	Description
group	VRRP group number
delay *seconds*	(Optional)Specifies the delay before a device declares itself master. The default value is 0.

Defaults

This function is disabled by default. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.

Command Mode

Interface configuration mode

Usage Guide

If the VRRP group is working in the preemption mode, once a device finds its priority is higher than the priority of the master, it will become the master device of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the master's priority, it will not become the master device of the VRRP group. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because that VRRP group has the highest priority and thus automatically becomes the master device in the VRRP group.

Configuration Examples

The following example enables IPv4 VRRP on interface GigabitEthernet 0/0.When VRRP group 1 finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 seconds.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)#vrrp 1 preempt delay 15
FS(config-if-GigabitEthernet 0/0)#vrrp 1 priority 200
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **priority** *level*	Sets the VRRP group priority.

Platform Description

N/A

1.9 vrrp priority

Use this command to specify the priority of the VRRP group.

Use the **no** form of this command to restore the default setting.

vrrp *group* **priority** *level*

no vrrp *group* **priority**

Parameter Description

Parameter	Description
group	VRRP group number
level	VRRP group priority

Defaults

This function is disabled by default. Once the VRRP function is enabled, the default priority of the VRRP group is 100.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the priority of IPv4 VRRP group 1 as 254.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **preempt** [**delay** *seconds*]	Sets the VRRP in the preemption mode.

Platform Description

N/A

1.10 vrrp timers advertise

Use this command to specify the interval for the master device to send the VRRP advertisement.

Use the **no** form of this command to restore the default setting.

vrrp *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

no vrrp *group* **timers advertise**

Parameter Description

Parameter	Description
group	VRRP group number
advertise-interval	Sets the interval time in seconds between sending VRRP advertisement.
csec *centisecond-interval*	Sets the interval time in milliseconds between sending advertisement frames from the master VRRP router in the backup group. The range is from 50 to 99. This value is not set by default.

Defaults

This function is disabled by default. Once the VRRP function is enabled, the default advertisement interval of the master device is one second.

Command Mode

Interface configuration mode

Usage Guide

If the current device becomes the master device in the VRRP group, it will notify its VRRP status, priority and other information by sending the VRRP advertisement in the set interval.

Configuration Examples

The following example sets the IPv4 VRRP advertisement interval as 4 seconds.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 4
```

The following example sets the IPv4 VRRP advertisement interval as 50 centi-seconds.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise csec 50
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp group timers learn	Enables the timer learning function.

Platform Description

N/A

1.11 vrrp timers learn

Use this command to enable the timer learning function.

Use the **no** form of this command to restore the default setting.

vrrp *group* **timers learn**

no vrrp *group* **timers learn**

Parameter Description

Parameter	Description
group	VRRP group number

Defaults

This function is disabled by default. Even if the VRRP function is enabled, the timer learning function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Once the timer learning function is enabled, if the current device is a VRRP backup device, it will learn the VRRP advertisement interval from the VRRP advertisement of the master device, with which it calculates the master device’s failure interval instead of the VRRP advertisement interval configured locally. This command may synchronize the VRRP advertisement timer with the master device.

Configuration Examples

The following example enables the timer learning function on the IPv4 VRRP group 1.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)#vrrp 1 timers learn
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **timers advertise** *interval*	Sets the IPv4 VRRP advertising interval.

Platform Description

N/A

1.12 vrrp track

Use these commands to enable the IPv4 VRRP track in the interface configuration mode. Use the **no** form of these commands to restore the default setting.

vrrp *group* **track** { *interface-type interface-number* } [*priority*]

no vrrp *group* **track** *interface-type interface-number*

Use these commands to enable VRRP IPv4 address track. Use the **no** form of these commands to restore the default setting.

vrrp *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

no vrrp *group* **track** *ipv4-address*

Parameter Description

Parameter	Description
group	VRRP group number
interface-type interface-number	Type of monitored interface
priority	VRRP priority change range when the interface or ip address reachability status changes. If this parameter is not selected, the default value is 10.
ipv4-address	Monitored IPv4 address. With BFD configured, it refers to the neighbor IP address.
interval *interval-value*	The interval of time to probe whether the monitored ip address is reachable or not. If this parameter is not selected, the default value is 3 seconds.
timeout *timeout-value*	The timeout time of the unreachable monitored ip address. If this parameter is not selected, the default value is 1 seconds.
retry *retry-value*	Track retries. If the value is reached, the link is thought unreachable. If this parameter is not configured, the default value is 3.

Defaults This function is disabled by default. Even if the VRRP function is enabled, no interface or IP address is specified.

Command Mode Interface configuration mode

Usage Guide

- ℹ This command can be used to monitor the outlet links. Note that layer-3 routable logical interfaces can be monitored (such as Routed Port, SVI and Loopback).
- ℹ If a host is monitored, specify the IPv4 address for the IPv4 VRRP router.
- ℹ If the host IP address is link-local, an interface must be specified.
- ℹ If a VRRP router owns the IP address of the physical interface, the priority is 255. Keep the priority when the monitored IP address or interface is set.

Configuration Examples The following example enables the VRRP group 1 to monitor the routed port Fa1/1. If the Fa1/1 link is disconnected, the priority of the VRRP group decreases by 30. When the Fa1/1 link recovers, the priority of VRRP group 1 is restored.

```
FS#configure terminal
FS(config)#interface    GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254
FS(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 1/1 30
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **priority** *level*	Sets the VRRP group priority.

Platform Description N/A

1.13 vrrp version

Use this command to configure the version of sending the IPv4 VRRP multicast packets.

For the IPv4 VRRP, there are two versions: VRRPv2 and VRRPv3.

Use the **no** form of this command to restore the default setting.

vrrp *group* **version** { **2** | **3** }

no vrrp *group* **version**

Parameter

Parameter	Description

Description

2	Uses the VRRPv2 version to send the packets.
3	Uses the VRRPv3 version to send the packets.

Defaults

The default is VRRPv2.

Command Mode

Interface configuration mode

Usage Guide

Considering the compatibility of VRRPv2 and VRRPv3 for the IPv4 VRRP, you can choose the version of VRRP packets based on the actual network environment. VRRPv2 is based on RFC3768 and VRRPv3 is based on RFC 5798.

ℹ This command is applicable to IPv4 VRRP only.

Configuration Examples

The following example configures the version of sending the IPv4 VRRP packets on the interface gi0/0.

```
FS#configure terminal
FS(config)#interface GigabitEthernet 0/0
FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch.
FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
FS(config-if-GigabitEthernet 0/0)# vrrp 1 version 3
```

Related Commands

Command	Description
vrrp *group* **ip** *ipaddress* [**secondary**]	Enables the VRRP function and set the IP address for the virtual device.
vrrp *group* **timers advertise** *interval*	Sets the interval of sending the VRRP advertisement.

Platform Description

N/A

2 RNS & Track Commands

2.1 delay

Use this command to specify a period of time after which the tracked object status will change if the interface status changes.

Use the **no** form of this command to restore the default setting.

delay { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }

no delay

Parameter Description

Parameter	Description
up *seconds*	Sets the delay time from down to up in the range from 0 to 180. The unit is second.
down *seconds*	Sets the delay time from up to down in the range from 0 to 180. The unit is second.

Defaults

There is no delay by default.

Command Mode

Track configuration mode

Usage Guide

The continual oscillation of the tracked object status may cause the client of this tracked object changing also. This command can be used to delay advertising the change of the tracked object status. For example, the status of a tracked object changes from up to down, if the delay down 180 is configured, the down status will be advertised after 180 seconds. If the tracked object status changes to the up again in this period, it won't be advertised. For the client of the tracked object, the status of the tracked object is always up.

Configuration Examples

The following example sets the delay time to 30 seconds when the tracked object changes to up from down.

```
FS(config)# track 5 rns 10
FS(config-track)# delay up 30
FS(config-track)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.2 dns

Use this command to set an IP RNS object to send the DNS packets and to enter the IP RNS DNS mode.

dns *destination-hostname* **name-server** *a.b.c.d* [**source-ipaddr** *ip-address*] [[**out-interface** *type num* [**next-hop**

A.B.C.D]] | [**af-direct out-interface** *type num* **next-hop** *A.B.C.D*]]

Parameter Description

Parameter	Description
destination-hostname	Sets the destination IP address or the destination host domain name.
oob	Enables management port detection.
a.b.c.d	Sets the IP address for the DNS server.
ip-address	Indicates the source IP address of RNS packets.
out-interface *type num*	Specifies the egress interface (non-management port) for RNS packets.
af-direct	Specifies the RNS object to directly receive the packets without passing through the protocol stack.
via *type num*	Specifies the management port as the egress interface (non-management port) for RNS packets.
A.B.C.D	Specifies the next-hop IP address for RNS packets.

Defaults N/A

Command Mode IP RNS configuration mode

Usage Guide Use this command to set an IP RNS object to send the DNS packets and to enter the IP RNS DNS mode. If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

Configuration Examples The following example sets the IP RMS object to send the DNS packets.

```
FS(config)# ip rns 1
FS(config-ip-rns)# dns www.FS.com.cn name-server 61.154.22.41
FS(config-ip-rns-dns)# exit
FS(config)# ip rns schedule 1 start-time now
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.3 frequency

Use this command to set the interval of sending the packets, which must be no smaller than the timeout time.

Use the **no** form of this command to restore the default setting.

frequency *milliseconds*

no frequency

Parameter Description

Parameter	Description
milliseconds	Sets the interval of sending the packets, in the range from10 to 604,800,000 in the unit of milliseconds.

Defaults

The default is 60 seconds.

Command Mode

IP RNS ICMP echo configuration mode
IP RNS DNS configuration mode

Usage Guide

Use this command to set the interval of sending the ICMP echo or DNS packets, which must accord with the following formula to ensure accuracy:

frequency *milliseconds* > **timeout** *milliseconds* >= **threshold** *millisecond*s

Configuration Examples

The following example configures an ICMP echo probe whose destination address is 192.168.21.1. The frequency, timeout time and threshold are set to 30,000, 8,000 and 6,000 milliseconds respectively.

```
FS(config-ip-rns)#icmp-echo 192.168.21.1
FS(config-ip-rns-icmp-echo)#frequency 30000
FS(config-ip-rns-icmp-echo)#timeout 8000
FS(config-ip-rns-icmp-echo)#threshold 6000
```

Related Commands

Command	Description
timeout	Defines the timeout time of sending the packets.

Platform Description

N/A

2.4 icmp-echo

Use this command to configure an ICMP echo RNS probe.

icmp-echo { *destination-ip-address* | *destination-hostname* [**name-server** *ip-address*] } [**source-ipaddr** *ip-address*] [[**out-interface** *type num* [**next-hop** *A.B.C.D*]] | [**af-direct out-interface** *type num* **next-hop** *A.B.C.D*]]

Parameter Description

Parameter	Description
destination-ip-address	Sets the destination IP address for the ICMP echo packets.
oob	Enables management port detection.
destination-hostname	Sets the destination host name within 127 characters. The exceeding characters are truncated automatically.
name-server *ip-address*	Sets the domain name server. The default domain name server is configured via the **ip name-server** command.

source-ipaddr *ip-address*	Sets the source IP address for the ICMP echo packets.
out-interface *type num*	Sets the egress port(non-management) for the probe packet.
af-direct	Specifies the RNS object to directly receive the packets without passing through the protocol stack.
via *type num*	Specifies the management port as the egress interface (non-management port) for probe packets.
next-hop *A.B.C.D*	Sets the next hop IP address.

Defaults

N/A

Command Mode

IP RNS configuration mode

Usage Guide

This command is used to enable the IP RNS object to send ICMP echo packets containing the specified destination IP address. The default payload size of an ICMP echo packet is 36 bytes. The **request-data-size** command is used to modify the packet size.

You can modify the probe parameter after specifying the type of the IP RNS probe (such as ICMP echo probe). If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

Configuration Examples

The following example enables the IP RNS object to send the ICMP echo packets containing the destination IP address 10.1.1.1.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 10.1.1.1
FS(config-ip-rns-icmp-echo)# exit
FS(config)# ip rns schedule 1 start-time now life forever
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.5 ip rns

Use this command to define an IP RNS operation object and to enter the IP RNS configuration mode.

Use the **no** form of this command to delete an IP RNS operation object.

ip rns *operation-number*

no ip rns *operation-number*

Parameter Description

Parameter	Description
operation-number	Sets the IP RNS operation object number, in the range from 1 to 500.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Use this command to define an IP RNS operation object and to enter the IP RNS configuration mode. At present, IP RNS probe only supports IPv4 upon 500 objects at most, which depends on device performance. As a value-added feature, too much IP RNS probe may lead in system overload. As a result, it will be disabled for the time being, ensuring normal function of core services (e.g. routing).

After the IP RNS configuration mode is enabled, the probe object will not be created unless the probe type is configured. If the type is set and object is created, use the **ip rns schedule** command to configure the startup policy, or the probe cannot be performed; use the **ip rns** command to enter the sub mode. If you want to change the probe type, you should delete the probe first by using the **no ip rns** command and then perform new configuration.

Configuration Examples

The following example defines the IP RNS object 1.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 10.1.1.1
FS(config-ip-rns-icmp-echo)# exit
FS(config)# ip rns schedule 1 start-time now life forever
```

Related Commands

Command	Description
show ip rns statistics	Displays the statistical data on the IP RNS object.

Platform Description

N/A

2.6 ip rns reaction-configuration

Use this command to configure proactive threshold monitoring and trigger for the IP RNS probe.

Use the **no** form of this command to restore the default setting.

ip rns reaction-configuration *operation-numbe*r **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]*
no ip rns reaction-configuration *operation-number* [**react** *monitored-element]*

Parameter Description

Parameter	Description
operation-number	Operation index, in the range from 1 to 500.
monitored-element	● Monitored element. The available parameters are listed as follows: ● **allfail**: Failed to monitor all elements. The default action-type is **track**. This parameter is applied on the track module for communication.

	● **rtt**: Packet round trip time (RTT) exceeds the threshold range. ● ·**timeout**: Timeout in whatever direction.
action-type *option*	● The available parameters include: ● **none**: No action, which is the default setting ● **trigge**r: Only supports the **trigger** action. ● **track**: Only supports the **track** action. Only when **monitored-element is allfail is this parameter supported, which is available exclusively.**
average **[** *number-of-measurements* **]**	Triggers operation when the average value of **number-of-measurements c**onsecutive times exceeds the threshold range. For example. *number-of-measurements* is set to three. Upper and lower thresholds are 5000 **and 4000 respectively. The average value for three consecutive measurements 6000. 6000. 5000 is (6000+6000+5000)/3=5667, exceeding the upper threshold 5000. The valid range is from 1 to 16 and the default is 5.**
consecutive [*occurrences* **]**	Triggers operation when the value of monitored element exceeds the threshold range for *occurrences* consecutive times. The valid range is from 1 to 16. The default is 5.
immediate	Triggers operation immediately when the value of monitored element exceeds the threshold range.
never	Never triggers operation.
xofy [x-value y-value]	X probes among the latest Y ones exceed the threshold range. The valid X range is from 1 to 16 and the default is 5. The valid Y range is from 1 to 16 and the default is 5.
threshold-value *upper-threshold lower-threshold*	Configures upper and lower thresholds. When *monitored-element* is **rtt,** this parameter indicates time, in the range from 0 to 60,000 milliseconds. See **Usage Guide** for the default setting. When react type is timeout, you don't need to configure this parameter.

Defaults N/A

Command Mode Global configuration mode

Usage Guide One IP RNS object can be configured with multiple thresholds monitoring, each for one element. Monitored elements that are supported vary with different probe types.

monitored-element	icmp-echo	dns
timeout		
rtt		

The default thresholds for monitored elements are listed as follows:

Monitored Element	Upper Threshold	Lower Threshold
timeout	-	-
rtt	5000 ms	0 ms

Configuration Examples

The following example configures RNS1 and its threshold monitoring.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 192.168.23.1
FS(config-ip-rns-icmp-echo)# exit
FS(config)# ip rns schedule 1 start-time now life forever
FS(config)#ip rns reaction-configuration 1 react timeout threshold-type immediate action-type triggerOnly
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.7 ip rns reaction-trigger

Use this command to enable the IP RNS probe which exceeds the monitoring threshold to trigger another IP RNS probe which is in the pending state.

Use the **no** form of this command to restore the default setting.

ip rns reaction-trigger *operation-number target-operation*

no ip rns reaction-trigger *operation-number target-operation*

Parameter Description

Parameter	Description
operation-number	The source operation number, in the range from 1 to 500
target-operation	The target operation number, in the range from 1 to 500

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

The trigger function is applied in network fault diagnosis scenario

Configuration Examples

The following example enables IP RNS1 to trigger IP RNS 2.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo www.baidu.com
FS(config-ip-rns-icmp-echo)# exit
FS(config)#ip rns schedule 1 start-time now life forever
FS(config)#ip rns reaction-configuration 1 react timeout threshold-type immediate action-type trigger
FS(config)# ip rns 2
FS(config-ip-rns)# dns www.baidu.com name-server 8.8.8.8
FS(config-ip-rns-dns)# exit
FS(config)#ip rns reaction-trigger 1 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.8 ip rns reset

Use this command to clear all IP RNS configuration.

ip rns reset

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to clear all IP RNS configuration. This command is used only in extreme cases (for example, RNS probe configuration is wrong).

Configuration Examples The following example clears all IP RNS configuration.

```
FS(config)# ip rns reset
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.9 ip rns restart

Use this command to restart the IP RNS probe.

ip rns restart *operation-number*

Parameter Description

Parameter	Description
operation-number	Sets the IP RNS operation object number, in the range from 1 to 500.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to restart the IP RNS probe whose schedule is in the pending state. This command is invalid for the IP RNS probe not configured with the scheduling policy.

Configuration Examples

The following example restarts IP RNS 1.

```
FS(config)# ip rns restart 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.10 ip rns schedule

Use this command to configure the scheduling strategy, start time and survival time for the IP RNS probe. Use the **no** form of this command to restore the default setting.

ip rns schedule operation-number [**life** { **forever** | *seconds* }] [**start-time** { *hh:mm* [*:ss*] [month *day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss* }] [**recurring**]

no ip rns schedule *operation-number*

Parameter Description

Parameter	Description
operation-number	RNS operation index, in the range from 1 to 500
life forever	The RNS operation is valid forever.
life *seconds*	The RNS survival time, measured in seconds
*hh***:***mm* [**:***ss* **]**	Defines the time when the operation starts,
month	The month when the operation starts, in the range from January (Jan.) to December (Dec.). The default is the current month.
day	The day when the operation starts, in the range from 1 to 31. The default is the current day.
pending	The start time is pending.
now	The operation starts right now.
after *hh:mm:ss*	The operation starts after hh hours, mm minutes and ss seconds.
recurring	The operation starts automatically as scheduled every day.

Defaults

The IP RNS probe is in the pending state by default. In other words, the probe is not performed unless it is triggered by another RNS probe.

Command Mode

Global configuration mode

Usage Guide

The **ip rns schedule** command is used to configure the IP RNS probe with scheduling policy. Once the scheduling policy is configured, the RNS probe cannot be modified. You can modify the RNS probe after deleting the schedule with the **no ip rns schedule** command.

Life {seconds} refers to the survival time of the IP RNS probe. The probe will end after the survival time.

Configuration Examples

The following example configures the RNS probe with scheduling policy.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 10.1.1.1
FS(config-ip-rns-icmp-echo)# exit
FS(config)#ip rns schedule 1 start-time now life forever
```

Once the scheduling policy is configured, the RNS probe cannot be modified. The RNS probe can be modified after the schedule is deleted.

```
FS(config)# ip rns 1
Entry already running and cannot be modified
          (only can delete (no) and start over)
          (check to see if the probe has finished exiting)
FS(config)# no ip rns schedule 1
FS(config)# ip rns 1
FS(config-ip-rns-icmp-echo)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.11 object

Use this command to add a tracked object to the object track list.

Use the **no** form of this command to delete a traced object.

object *object-number* [**not**]

no object *object-number*

Parameter Description

Parameter	Description
object-number	Tracked object number, in the range from 1 to 700

Defaults

No tracked object is configured by default.

Command

Track configuration mode

Mode

Usage Guide This command is used to add a tracked object to the object track list. The number of tracked objects is only restricted by the track list capacity.

object *object-number*: The tracked object must be in the up state for the track list to be in the up state.

object *object-number* not: track: The tracked object must be in the up state for the track list to be in the up state,

- This command is configured only in track configuration mode for the track list.
- The object cannot track itself.
- The objects cannot track each other. For example, if A tracks B, B cannot track A. Otherwise, both A and B are in oscillation.

Configuration Examples The following example adds tracked object 4 to the object track list. When object 1 is in the up state, 2 down, 3 up, object 4 is in the up state.

```
FS(config)# track 4 list boolean and
FS(config-track)# object 1
FS(config-track)# object 2 not
FS(config-track)# object 3
FS(config-track)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.12 request-data-size

Use the following example to set the protocol payload size of IP RNS probe packet.

Use the **no** form of this command to restore the default setting.

request-data-size *bytes*

no request-data-size

Parameter Description

Parameter	Description
bytes	The number of payload bytes. The minimum/maximum number of bytes varies with the probe type.

Defaults The default is the minimum payload byte, which varies with the probe type.

Command Mode IP RNS ICMP echo configuration mode

Usage Guide

This command is used to fill bytes in the probe packet to probe for the bigger packet.

Probe Type	Range	Default
icmp-echo	[36, 1472]	36

Configuration Examples

The following example sets the protocol payload size of the IP RNS probe packet to 50.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 10.1.1.1
FS(config-ip-rns-icmp-echo)# request-data-size 50
FS(config-ip-rns-icmp-echo)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.13 show ip rns collection-statistics

Use this command to display statistics about the RNS probe.

show ip rns collection-statistics [*operation-number*]

Parameter Description

Parameter	Description
operation-number	Sets the IP RNS operation object number, in the range from 1 to 500. The default is all IP RNS operation objects.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display statistics about an IP RNS probe.

Configuration Examples

The following example displays statistics about the all RNS probes.

```
FS#show ip rns collection-statistics 1
Entry number: 1
Start Time Index: *2014-03-20 19:53:51
Number of successful operations: 919
Number of operations over threshold: 0
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 2
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 2
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
RTT Values:
RTTAvg: 18          RTTMin: 16          RTTMax: 37
NumOfRTT: 919       RTTSum: 16654       RTTSum2: 302786
```

Field	Description
Entry number	IP RNS operation index
Start Time Index:	Schedule start time
Number of successful operations:	Number of successful operation.
Number of operations over threshold:	Number of threshold violation
Number of failed operations due to a Disconnect:	Number of operation failure due to disconnection
Number of failed operations due to a Timeout:	Number of operation failure due to timeout
Number of failed operations due to a Busy:	Number of operation failure since the peer end is busy
Number of failed operations due to a No Connection:	Number of operation failure due to no connection
Number of failed operations due to an Internal Error:	Number of operation failure due to internal error
Number of failed operations due to a Sequence Error:	Number of operation failure due to sequence error
Number of failed operations due to a Verify Error:	Number of operation failure due to verification error
RTT Values	RTT value
RTTAvg:	Average RTT value
RTTMin:	Minimum RTT value
RTTMax:	Maximum RTT value
NumOfRTT:	Number of counting RTT value
RTTSum:	Sum of RTT value
RTTSum2:	Sum of squares of RTT value

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.14 show ip rns configuration

Use this command to display the RNS instance configuration.

show ip rns configuration [*operation-number*]

Parameter Description

Parameter	Description
operation-number	Sets the RNS instance number, in the range from 1 to 500.

Command

Privileged EXEC mode

Mode

Usage Guide This command is used to display the RNS instance configuration. The configuration varies with different packet types.

Configuration Examples The following example displays the RNS 1 configuration.

```
FS# show ip rns configuration 1
Entry number: 1
Tag: FS555
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 10000
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
```

Field	Description
Entry number	IP RNS operation index
Tag	Instance tag.
Type of operation to perform	Operation type.
Operation timeout (milliseconds)	Operation timeout.
Operation frequency (milliseconds)	Operation frequency.
Threshold (milliseconds)	Threshold.
Recurring (Starting Everyday)	The operation starts every day.
Life (seconds)	Life time
Next Scheduled Start Time	Next scheduled start time.
Target address/Source address	Target address/Source address
Request size (ARR data portion)	Request packet size.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.15 show ip rns operational-state

Use this command to display operational state.

show ip rns operational-state [*operation-number*]

Parameter

Parameter	Description

Description

operation-number	Sets the IP RNS operation object number, in the range from 1 to 500. The default is all RNS operation objects.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the state information about an RNS probe.

Configuration Examples

The following example displays the state information about all RNS probes.

```
FS# show ip rns operational-state
Entry number: 1
Modification time: *2014-01-10 10:26:14
Current seconds left in Life: Forever
Operational state of entry: Active
Number of Octets Used by this Entry: 2272
Number of operations attempted: 232
Number of operations skipped: 0
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 4
Latest operation start time: 2014-01-10 10:26:55
Latest operation return code: OK
```

Field	**Description**
Entry number	IP RNS operation index
Modification time	Probe result recounting time (every time schedule is enabled, the result is counted again).
Number of Octets Used by this Entry	Number of octets contained in the probe packet.
Number of operations attempted	Number of attempted operation.
Number of operations skipped	Number of failed operation.
Current seconds left in Life	Probes for the left life.
Operational state of entry	Probes for the operational state (Active/Disactive).
Connection loss occurred	Connection loss occurred.
Timeout occurred	Send request timeout occurred,
Over thresholds occurred	Threshold violation occurred.
Latest RTT (milliseconds)	Latest RTT.
Latest operation start time	Latest operation start time.
Latest operation return code	Latest operation return code.

Related

Command	**Description**

Commands

N/A	N/A

Platform Description

N/A

2.16 show ip rns reaction-configuration

Use this command to display the proactive threshold monitoring information of an IP RNS probe.

show ip rns reaction-trigger [*operation-number*]

Parameter Description

Parameter	Description
operation-number	The number of IP RNS operation objects, in the range from 1 to 500. The default is all RNS operation objects.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the proactive threshold monitoring information of an IP RNS probe.

Configuration Examples

The following example displays the proactive threshold monitoring information of all IP RNS probes.

```
FS#show ip rns reaction-configuration
Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: trigger
Reaction: timeout
Threshold Type: Never
Threshold Count: 5
Threshold Count2: 5
Action Type: trigger
```

Field	Description
Entry number	IP RNS operation index
Reaction	Monitored object
Threshold Type	The available parameters are listed as follows: **never**: Never triggers operation. **consecutive**: Triggers operation when the value of

	monitored element exceeds the threshold range for *occurrences* consecutive times. **average**: Triggers operation when the average value of **number-of-measurements consecutive times** exceeds the threshold range. **immediate**: Triggers operation immediately when the value of monitored element exceeds the threshold range. **xofy:** X probes among the latest Y ones exceed the threshold range.
Rising (milliseconds)	Upper threshold
Falling (milliseconds)	Lower threshold
Threshold Count	The parameter refers to the x value when the threshold-type is **xofy** or the average count when the threshold-type is **average**.
Threshold Count2	The parameter refers to the y value when the threshold-type is **xofy** or the consecutive count when the threshold-type is **consecutive**.
Action Type	Action type

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.17 show ip rns reaction-trigger

Use this command to display the reaction trigger information for all RNS objects.

show ip rns reaction-trigger [*operation-number*]

Parameter Description

Parameter	Description
operation-number	The number of IP RNS operation object, in the range from 1 to 500. The default is all RNS operation objects.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display the reaction trigger information for all RNS objects.

Configuration Examples

The following example displays the reaction trigger information for all RNS objects.

```
FS#show ip rns reaction-trigger
Entry number: 1
Target rns index: 2
Status of Entry (SNMP RowStatus): active
Operational State: pending
```

Field	Description
Entry number	RNS index
Target rns index	Target RNS index
Status of Entry (SNMP RowStatus)	Status of RNS entry
Operational State	Reaction-trigger state

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.18 show ip rns statistics

Use this command to display the RNS object statistics.

show ip rns statistics [*operation-number*]

Parameter Description

Parameter	Description
operation-number	Sets the IP RNS operation object number, in the range from 1 to 500

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

The statistics vary with different packet types.

Configuration Examples

The following example displays the RNS object statistics.

```
FS#show ip rns statistics 1
Round trip time(RTT) Index 1
Operation time to live: Forever
Latest RTT: 1 ms
Latest operation start time: 2014-01-20 10:21:38
Latest operation return code: OK
Number of successes: 386
Number of failures: 12
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.19 show track

Use this command to display statistics of the tracked object.

show track [*track-number*]

Parameter Description

Parameter	Description
track-number	Sets the tracked object number, in the range from 1 to 700.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays statistics of all tracked objects.

```
FS#show track
Track 1
  Reliable Network Service 5
  The state is Up
    1 change, current state last: 120 secs
  Delay up 30 secs, down 50 secs
Track 3
  Interface FastEthernet 1/0
  The state is Down, delayed Up (5 secs remaining)
    3 change, current state last: 300 secs
  Delay up 60 secs, down 60 secs
Track 4
  List boolean and
   Object 1
   Object 2 not
  The state is Up
   1 change, current state last: 100 secs
   Delay up 0 secs, down 0 secs
```

Field	Description
Track x	Tracked object ID
Reliable Network Service x	Tracked RNS object
The state is x	Tracked object state
x change	Tracked object change count
current state last: x secs	The time for which the current state lasts
Delay up x secs, down x secs	The delay state of the tracked object
Interface x x	Tracked interface
The state is x, delayed y (c secs remaining)	The tracked object state is x, and will turn to y in c seconds.
List boolean and	The Boolean expression enables calculation by using “and” operator.
Object x	Object x is in the up state.
Object x not	Object x is in the down state.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.20 show track client

Use this command to display the track client statistics.

show track client

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the statistics of the client connecting to track.

Configuration Examples

The following example displays the statistics of the client connecting to track.

```
FS# show track client
Track client 2: socket 4
client_path: /tmp/vsd/0/track/.client_nsm
Connection time: Fri Dec 28 17:04:43 2012
```

Field	Description
Track client x: socket x	Track client number and socket
client_path: /tmp/vsd/0/track/.client_nsm	The path from the client to track
Connection time: xx xx xx xx:xx:xx xx	The time when the client connects to track

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.21 tag

Use this command to set the tag for IP RNS probe.

Use the **no** form of this command to restore the default setting.

tag *text*

no tag

Parameter Description

Parameter	Description
text	Sets the tag for IP RNS probe, which is composed of up to 79 printable characters.

Defaults

N/A

Command Mode

IP RNS DNS configuration mode

IP RNS ICMP echo configuration mode

Usage Guide

Tag is used to identify the probe. When the tag exceeds 79 characters, the surplus characters are truncated.

Configuration Examples

The following example sets the tag for IP RNS probe to telecom gateway.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 10.1.1.1
FS(config-ip-rns-icmp-echo)# tag telecom_gateway
FS(config-ip-rns-icmp-echo)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.22 threshold

Use this command to configure the upper threshold value for IP RNS probe.

Use the **no** form of this command to restore the default setting.

threshold *milliseconds*

no threshold

Parameter Description

Parameter	Description
milliseconds	Sets the upper threshold value, in the range from 0 to 60,000 in the unit of milliseconds.

Defaults

The default is 5,000 milliseconds.

Command Mode

IP RNS DNS configuration mode

IP RNS ICMP echo configuration mode

Usage Guide

The threshold value must be no greater than the timeout value. See **Usage Guide** of the **frequency** command for the relationship among timeout, frequency and threshold.

Configuration Examples

The following example sets the upper threshold value for IP RNS probe to 8,000 milliseconds.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 10.1.1.1
FS(config-ip-rns-icmp-echo)# threshold 8000
FS(config-ip-rns-icmp-echo)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.23 timeout

Use this command to set the timeout time of an IP RNS probe.

Use the **no** form of this command to restore the default setting.

timeout *milliseconds*

no timeout

Parameter Description

Parameter	Description
milliseconds	Sets the timeout time, in the range from 10 to 604,800,000 in the unit of

	milliseconds. The default is 5,000 milliseconds.

Defaults

The default timeout of an IP RNS probe varies with the detection type, which can be displayed by using **show ip rns configuration** command.

Command Mode

IP RNS ICMP echo configuration mode
IP RNS DNS configuration mode

Usage Guide

The timeout value must be no smaller than the threshold value. See **Usage Guide** of the **frequency** command for the relationship among timeout, frequency and threshold.

Configuration Examples

The following example sets the timeout time of an IP RNS probe to 10,000 milliseconds.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 10.1.1.1
FS(config-ip-rns-icmp-echo)# timeout 10000
FS(config-ip-rns-icmp-echo)# exit
```

Related Commands

Command	Description
frequency *milliseconds*	Sets the interval of sending the packets.

Platform Description

N/A

2.24 tos

Use this command to set the Type of Service (ToS) field in the IPv4 header of an IP RNS probe packet.

Use the **no** form of this command to restore the default setting.

tos *number*

no tos

Parameter Description

Parameter	Description
number	Sets the ToS field in the IPv4 header of an IP RNS probe packet, in the range from 0 to 255.

Defaults

The default is 0.

Command Mode

IP RNS DNS configuration mode
IP RNS ICMP echo configuration mode

Usage Guide

ToS is an 8-bit field of an IPv4 packet. ToS can be used to set probe packet priority. Different ToS corresponds to different priority.

Configuration Examples

The following example sets the ToS field in the IPv4 header of an IP RNS probe packet to 128.

```
FS(config)# ip rns 1
FS(config-ip-rns)# icmp-echo 10.1.1.1
FS(config-ip-rns-icmp-echo)# tos 128
FS(config-ip-rns-icmp-echo)# exit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.25 track interface line-protocol

Use this command to configure a tracked object to track the interface status and enter the track mode.

Use the **no** form of this command to delete a tracked object.

track *object-number* **interface** *interface-type interface-number* **line-protocol**

no track *object-number*

Parameter Description

Parameter	Description
object-number	Sets the tracked object number, in the range of 1 to 700.
interface-type interface-number	Sets the interface type and the interface number.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to configure a tracked object to track the link state of the interface. If the link state of the interface is up, the state of the corresponding tracked object is up too.

Configuration Examples

The following example configures the object “track 3” to track the link state of ethernet 0/1.

```
FS(config)# track 3 interface ethernet 0/1 line-protocol
```

Related Commands

Command	Description
track rns	Configures a tracked object to track the operating status of an rns object.
show track	Displays the tracked object related information.

Platform Description

N/A

2.26 track list

Use this command to configure a tracked list object and specify the state of the tracked list based on a Boolean calculation.

Use the **no** form of this command to restore the default setting.

track *object-number* **list boolean { and | or }**

no track *object-number*

Parameter Description

Parameter	Description
object-number	Sets the number of the tracked object, in the range from 1 to 700.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to configure a tracked list object and specify the state of the tracked list based on a Boolean calculation

- **track** *object-number* **list boolean and:** Configure a tracked list with a Boolean expression using “AND” operator.
- **track** *object-number* **list boolean or**: Configure a tracked list with a Boolean expression using “OR” operator.

Configuration Examples

The following example configures tracked list object “4” and specifies the state of the tracked list based on a Boolean calculation using operator “AND”.

```
FS(config)# track 4 list boolean and
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.27 track rns

Use this command to configure a tracked object to track the operating status of an RNS object and enter the track mode.

Use the **no** form of this command is used to delete a tracked object.

track *object-number* **rns** *entry-number*

no track *object-number*

Parameter Description

Parameter	**Description**
object-number	Sets the tracked object number, in the range from 1 to 700.
entry-number	Sets the RNS object number, in the range from 1 to 500.

Defaults N/A

Command Mode Global configuration mode

Usage Guide The RNS object status is determined by whether the response packets are received. If so, the RNS object status is up and the status of the corresponding tracked object that tracks this RNS is also up.

Configuration Examples The following example configures the object “track 5” to track the RNS instance “rns 7”.

```
FS(config)# track 5 rns 7
```

Related Commands

Command	**Description**
track interface line-protocol	Tracks the status of one interface and enter the track mode.
show track [*track-number*]	Displays the tracked object related information.

Platform Description N/A

Chapter 10 Routing Commands

1. PBR Commands
2. Route-DB Commands
3. RIP Commands
4. RIPNG Commands
5. OSPFv2 Commands
6. OSPFv3 Commands
7. Protocol-independent Commands
8. NSM Commands

1 PBR Commands

1.1 clear ip pbr statistics

Use this command to clear the IPv4 PBR forwarded packet count.

clear ip pbr statistics [**interface** *if-name* **|** **local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the device clears the IPv4 PBR forwarded packet count on that interface. Otherwise, the device clears the IPv4 PBR forwarded packet count on every interface where IPv4 PBR is enabled.
local	Clears the IPv4 PBR forwarded packet count on the local interface.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

Use this command to clear the IPv4 PBR forwarded packet count.

Configuration Examples

The following example clears the IPv4 PBR forwarded packet count.

```
FS#clear ip pbr statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.2 clear ipv6 pbr statistics

Use this command to clear the IPv6 PBR forwarded packet count.

clear ipv6 pbr statistics [**interface** *if-name* **|** **local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the device clears the IPv6 PBR forwarded packet count on that interface. Otherwise, the device clears the IPv6 PBR forwarded packet count on every interface where IPv6 PBR is enabled.
local	Clears the IPv6 PBR forwarded packet count on the local interface.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide Use this command to clear the IPv6 PBR forwarded packet count.

Configuration Examples The following example clears the IPv6 PBR forwarded packet count.

```
FS#clear ipv6 pbr statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.3 ip local policy route-map

Use this command to apply the policy-based routing (PBR) on the packets sent locally. Use the **no** form of this command to restore the default setting.

ip local policy route-map *route-map-name*

no ip local policy route-map

Parameter Description

Parameter	Description
route-map-name	Name of the route map

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

The **set interface** command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.

Configuration The following examples send the packets with the source address 192.168.217.10 from the serial 2/0.

Examples

The following example defines an ACL that match the IP packet.

```
FS(config)#access-list 1 permit 192.168.217.10
```

The following example defines the route map.

```
FS(config)#route-map lab1 permit 10
FS(config-route-map)#match ip address 1
FS(config-route-map)#set interface serial 2/0
FS(config-route-map)#exit
```

The following example applies PBR on the local interface.

```
FS(config)#ip local policy route-map lab1
```

Related Commands

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the output port of the policy-based routing.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform Description

N/A

1.4 ip policy

Use this command to set the policy: redundant backup or load balancing used between multiple next hops of the PBR applied for the **set ip [default] nexthop** command in global configuration mode. Use the **no** form of this command to restore the default setting.

ip policy { **load-balance** | **redundance** }

no ip policy

Parameter Description

Parameter	Description
load-balance | redundance	Specifies the policy: load balancing or redundant backup.

Defaults

Redundant backup is adopted by default.

Command Mode

Global configuration mode

Usage Guide

When you configure the **set ip next-hop** command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop of the policy-based routing takes effect. When the load balancing is set, multiple resolved next hops of the policy-based routing take effect. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops. The resolved next hop refers to the ARP message learned by the next hop and the MAC address corresponding to this ARP exists in the MAC address table.

⚠ NPE80 does not support this command.

Configuration Examples

In the example below, there are multiple next hops configured in the route map. After the redundant backup is set in global configuration mode, only the first next hop among the sub-route map of the policy-based routing applied on the interface FastEthernet 0/0 takes effect.

The following example sets the ACL that match the IP packet.

```
FS(config)#access-list 1 permit 10.0.0.1
FS(config)#access-list 2 permit 20.0.0.1
```

The following example defines the route map.

```
FS(config)#route-map lab1 permit 10
FS(config-route-map)#match ip address 1
FS(config-route-map)#set ip next-hop 196.168.4.6
FS(config-route-map)#set ip next-hop 196.168.4.7
FS(config-route-map)#set ip next-hop 196.168.4.8
FS(config-route-map)#exit
FS(config)#route-map lab1 permit 20
FS(config-route-map)#match ip address 2
FS(config-route-map)#set ip next-hop 196.168.5.6
FS(config-route-map)#set ip next-hop 196.168.5.7
FS(config-route-map)#set ip next-hop 196.168.5.8
FS(config-route-map)#exit
```

The following example applies the policy-based routing on the interface.

```
FS(config)#interface FastEthernet 0/0
FS(config-if)#ip policy route-map lab1
FS(config-if)#exit
FS(config)#ip policy redundance
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.5 ip policy route-map

Use this command to apply the policy-based routing on an interface. Use the **no** form of this command to restore the default setting.

ip policy route-map *route-map*

no ip policy route-map

Parameter Description

Parameter	Description
route-map	Name of the route map

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

⚠ Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration Examples In the example below, when the interface FastEthernet0/0 receives a datagram, if the source address of the datagram is 10.0.0.1, it sets the next-hop as 196.168.4.6; if the source address is 20.0.0.1, it sets the next-hop as 196.168.5.6;, otherwise, the general forwarding will be performed.

The following example sets the ACL matched with the IP packets.

```
FS(config)#access-list 1 permit 10.0.0.1
FS(config)#access-list 2 permit 20.0.0.1
```

The following example defines the route map.

```
FS(config)#route-map lab1 permit 10
FS (config-route-map)#match ip address 1
FS(config-route-map)#set ip next-hop 196.168.4.6
FS(config-route-map)#exit
FS(config)#route-map lab1 permit 20
FS(config-route-map)#match ip address 2
FS(config-route-map)#set ip next-hop 196.168.5.6
FS(config-route-map)#exit
```

The following example applies the route map on the interface.

```
FS(config)#interface FastEthernet 0/0
FS(config-if)#ip policy route-map lab1
FS(config-if)#exit
```

Related Commands

Command	Description
access-list	Defines the access list rule.
route-map	Defines the route map.
set vrf	Defines the VRF instance of the policy-based IP packet.
set ip next-hop	Defines the next hop of the policy-based routing.
set ip default next-hop	Defines the default next hop of the policy-based routing.
set interface	Defines the policy-based routing output port.
set default interface	Defines the default policy-based routing output port.
set ip tos	Sets the TOS in the head of the IP packet.
set ip dscp	Sets the DSCP of the IP packet.
set ip precedence	Sets the priority level in the head of the IP packet.
match ip address	Sets the filtering rule.
match length	Matches the packet length.

Platform Description N/A

1.6 ipv6 local policy route-map

Use this command to enable the policy-based routing on the packets sent locally. Use the **no** form of this command to restore the default setting.

ipv6 local policy route-map *route-map-name*

no ipv6 local policy route-map

Parameter Description

Parameter	Description
route-map-name	Name of the router map applied locally, which is configured by the **router-map** command.

Defaults This function is disabled by default.

Command Mode Global Configuration mode

Usage Guide

- This command is valid only for the IPv6 packets in accordance with the policy (for example, ping packets used for management) sent locally, but not the packets received locally.

- To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

Configuration Examples

The following examples display the PBR application process: The device sends the packets from the source address 2003:1000::10/80 to the 2001:100::/64, the packets will match ACL6 of aaa and be sent to the device 2003:1001::2.

- The following example defines the ACL matched with the IPv6 packet:

```
FS(config)#ipv6 access-list aaa
FS(config)#permit ipv6 2003:1000::10/80 2001:100::/64
```

- The following example defines the router map.

```
FS(config)#route-map pbr-aaa permit 10
FS(config-route-map)#match ipv6 address aaa
FS(config-route-map)#set ipv6 next-hop 2003::1001::2
```

- The following example applies the PBR on the device.

```
FS(config)#ipv6 local policy route-map pbr-aaa
```

Related Commands

Command	Description
match ipv6 address	Sets the ACL6 used to match the IPv6 packets in the IPv6 PBR.
match length	Defines the length of matched packets.
route-map	Defines the route map for PBR.
set default interface	Defines the default next hop output port.
set interface	Defines the next hop output port.
set ipv6 default next-hop	Sets the default next hop of packet forwarding.
set ipv6 next-hop	Sets the next hop of packet forwarding.
set ipv6 precedence	Sets the priority field in the head of IPv6 packets.
show ipv6 policy	Displays the current PBR application.
show route-map	Displays the current router map configuration.

Platform Description

N/A

1.7 ipv6 policy

Use this command to set the policy: redundant backup or load balancing, applied for the **set ip nexthop** command in global configuration mode. Use the **no** form of this command to restore the default setting.

ipv6 policy { load-balance | redundance }

no ipv6 policy

Parameter Description

Parameter	Description
load-balance	Sets the policy as load balancing.
redundance	Sets the policy as redundant backup.

Defaults

Redundant backup is adopted by default.

Command Mode

Global configuration mode

Usage Guide

This function is valid for the multiple next-hops.

When you configure the set ip next-hop command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop takes effect. The second configured next hop will take effect only when the first one fails and the first next hop will take effect again if it recovers.

When the load balancing is set, multiple next hops of the policy-based routing take effect.

The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops.

⚠ The resolved next hop refers to the learned MAC address for the next-hop.

Configuration Examples

The following example sets load-balancing mode for multiple nexthops.

Step 1: configures an ACL matching with IP packets.

```
FS(config)# ipv6 access-list 1
FS(config-ipv6-acl )# permit ipv6 1000::1 any
FS(config)# ipv6 access-list 2
FS(config-ipv6-acl )# permit ipv6 2000::1 any
```

Step 2: defines a route map.

```
FS(config)# route-map lab1 permit 10
FS(config-route-map)# match ipv6 address 1
FS(config-route-map)# set ipv6 next-hop 2002::1
FS(config-route-map)# set ipv6 next-hop 2002::2
FS(config-route-map)# set ipv6 next-hop 2002::3
FS(config-route-map)# exit
FS(config)# route-map lab1 permit 20
FS(config-route-map)# match ipv6 address 2
FS(config-route-map)# set ipv6 next-hop 2002::5
FS(config-route-map)# set ipv6 next-hop 2002::6
FS(config-route-map)# set ipv6 next-hop 2002::7
FS(config-route-map)# exit
```

Step 3: applies policy-based routing on the interface.

```
FS(config)# interface FastEthernet 0/0
FS(config-if)# ipv6 policy route-map lab1
FS(config-if)# exit
FS(config)# ipv6 policy load-balance
```

Related Commands

Command	Description
set ipv6 default next-hop	Defines the default next hop for forwarding the packets.
set ipv6 next-hop	Defines the next hop for forwarding the packets.
show ipv6 policy	Displays the current policy-based routing application.

Platform Description

N/A

1.8 ipv6 policy route-map

Use this command to apply the policy-based routing on an interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

ipv6 policy route-map *route-map-name*

no ip policy route-map

Parameter Description

Parameter	Description
route-map-name	Name of the PBR router map applied locally, which is configured by the **router-map** command.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

⚠ Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration Examples

An IPv6 packet is received on the fastEthernet 0/0. If the packet is sent from 10::/64 network segment, it is forwarded to the next hop of 2000:1; if the packet is sent from 20::/64 network segment, it is forwarded to the next hop of 2000:2 or forwarded as usual.

Step 1: configures an ACL matched with the IP packet.

```
FS(config)# ipv6 access-list acl_for_pbr1
FS (config-ipv6-acl)# permit ipv6 10::/64    any
FS(config)# ipv6 access-list acl_for_pbr2
FS (config-ipv6-acl)# permit ipv6 20::/64    any
```

Step 2: defines a route map.

```
FS(config)# route-map rm_pbr    permit 10
FS (config-route-map)# match ipv6 address acl_for_pbr1
FS(config-route-map)# set ipv6 next-hop 2000::1
FS(config-route-map)# exit
FS(config)# route-map rm_pbr    permit 20
FS(config-route-map)# match ipv6 address acl_for_pbr2
FS(config-route-map)# set ipv6 next-hop 2000::2
FS(config-route-map)# exit
```

Step 3: applies the route map to the interface.

```
FS(config)# interface FastEthernet 0/0
FS(config-if)# no switchport
FS(config-if)# ipv6 policy route-map rm_pbr
FS(config-if)# exit
```

Related Commands

Command	**Description**
route-map	Defines the route map.
match ipv6 address	Sets the IPv6 ACL used to match the IPv6 packets in the IPv6 PBR.
set ipv6 default next-hop	Defines the default next hop of the packet forwarding.
set ipv6 next-hop	Defines the next hop of the packet forwarding.
show ipv6 policy	Displays the current policy-based routing application.
show route-map	Displays the current route map configurations.

Platform Description

N/A

1.9 show ip pbr route

Use this command to display the IPv4 PBR information on the interface.

show ip pbr route [**interface** *if-name* **|** **local**]

Parameter Description

Parameter	**Description**
interface *if-name*	Specifies the interface name. If the interface name is specified, the IPv4 BPR information of this interface is displayed. Otherwise, the IPv4 BPR information of all interfaces where the IPv4 PBR is enabled is displayed.

local	Displays the IPv4 PBR information on the local interface

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to display the IPv4 PBR information.

Configuration Examples The following example displays the IPv4 PBR information on the interfaces.

```
FS#show ip pbr route
PBR IPv4 Route Summay : 1
Interface              : GigabitEthernet 0/1
   Sequence             : 10
   ACL[0]               : 2900
ACL_CLS[0]          : 0
   Min Length          : None
   Max Length          : None
   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
```

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
Min Length	The minimum match length.
Max Length	The maximum match length.
Route Flags	PBR flag bit: Route Type: "PBR" indicates PBR routes. "Normal" indicates common routes.

	Direct: PBR matching action, **permit** or **deny** Priority: PBR priority, **High** or **Low** Tos_Dscp: Displays whether the **tos** rule or the **dscp** rule is configured. Precedence: Displays whether the **set ip precedence** rule is configured.
Mode	Specifies the redundancy mode or the next hop load balancing mode.
Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
Nexthop	Specifies the next hop IP address.
Weight	Specifies the next hop weight.
Ifindex	Specifies the outbound interface index corresponding to the next hop.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.10 show ip pbr route-map

Use this command to display the IPv4 PBR route-map information.

show ip pbr route-map *route-map-name*

Parameter Description

Parameter	Description
route-map-name	The route-map name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.11 show ip pbr statistics

Use this command to display the IPv4 PBR forwarded packet count.

show ip pbr statistics [**interface** *if-name* **|** **local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the IPv4 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv4 PBR forwarded packet count of all interfaces where the IPv4 PBR is enabled is displayed.
local	Displays the IPv4 PBR forwarded packet count on the local interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the IPv4 PBR forwarded packet count.

```
FS#show ip pbr statistics
IPv4 Policy-based route statistic
  gigabitEthernet 0/1
      statistics : 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.12 show ip policy

Use this command to display the interface configured with the policy-based routing and the name of route map applied on the interface.

show ip policy [*route-map-name*]

Parameter Description

Parameter	Description
route-map-name	Indicates the name of a route map.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

You can use this command to verify the current PBR configured in the system.

Configuration Examples

The following example displays the current PBR configured in the system.

```
FS#show ip policy
Banlance Mode: redundance
Interface                  Route map
local                        test
FastEthernet 0/0     test
```

Related Commands

Command	Description
ip policy route-map	Applies the policy-based routing on the interface.
ip local policy route-map	Applies the policy-based routing on the local interface.

Platform Description

N/A

1.13 show ipv6 pbr route

Use this command to display the IPv6 PBR information on the interface.

show ipv6 pbr route [**interface** *if-name* **|** **local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the IPv6 BPR information of this interface is displayed. Otherwise, the IPv6 BPR information of all interfaces where the IPv6 PBR is enabled is displayed.
local	Displays the IPv6 PBR information on the local interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration

The following example displays the IPv6 PBR information on the interfaces.

Examples

```
FS#show ipv6 pbr route
PBR IPv6 Route Summary : 1
Interface       : GigabitEthernet 0/2
  Sequence        : 10
  ACL[0]         : 2901
ACL_CLS[0]     : 0
  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]    : 10::1
   Weight[0]     : 1
   Ifindex[0]   : 3
```

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
Min Length	The minimum match length.
Max Length	The maximum match length.
VRF ID	Port associated VRF ID.
Route Flags	PBR flag bit: Route Type: “PBR” indicates PBR routes. “Normal” indicates common routes. Direct: PBR matching action, **permit** or **deny** Priority: PBR priority, **High** or **Low** Tos_Dscp: Displays whether the **tos** rule or the **dscp** rule is configured. Precedence: Displays whether the **set ip precedence** rule is configured.
Mode	Specifies the redundancy mode or the load balance mode for the next hop.

Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
Nexthop	Specifies the next hop IP address.
Weight	Specifies the next hop weight.
Ifindex	Specifies the outbound interface index corresponding to the next hop

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.14 show ipv6 pbr route-map

Use this command to display the IPv6 PBR route-map information.

show ipv6 pbr route-map *route-map-name*

Parameter Description

Parameter	Description
route-map-name	The route-map name.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the IPv6 PBR route-map information.

```
FS#show ipv6 pbr route-map rm6
Pbr VRF: GLOBAL, ID: 0
  Forward Mode: redundance
  Forwarding: On

route-map rm6
    route-map index: sequence 10, permit
Match rule:
    ACL ID :            0, ACL CLS: 0, Name: acl6
        Set rule:
            IPv6 Nexthop: 10::1, (VRF Name: , ID: 0), Weight: 0, Flags: 0
            PBR state info ifx: GigabitEthernet 0/0, Connected: true, Track State: valid, Flags: 0
```

Field	Description
Pbr VRF	VRF name and VRF ID.
Forward Mode	Sets the load balancing mode or to the redundancy mode for the next hop.
Forwarding	Displays whether the IP route forwarding is enabled.
Route-map index	The serial number and the type of the sub-map.
Match rule	Match rule
Set rule	Set rule.
PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.15 show ipv6 pbr statistics

Use this command to display the IPv6 PBR forwarded packet count.

show ip pbr statistics [**interface** *if-name* **|** **local**]

Parameter Description

Parameter	Description
interface *if-name*	Specifies the interface name. If the interface name is specified, the IPv6 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv6 PBR forwarded packet count of all interfaces where the IPv6 PBR is enabled is displayed.
local	Displays the IPv6 PBR forwarded packet count on the local interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the IPv6 PBR forwarded packet count.

```
FS#show ipv6 pbr statistics
IPv6 Policy-based route statistic
  gigabitEthernet 0/1
      statistics : 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.16 show ipv6 policy

Use this command to display which interfaces are configured with IPv6 PBR.

show ipv6 policy [*route-map-name*]

Parameter Description

Parameter	Description
route-map-name	Name of the PBR router map.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the current PBR applied in the system.

```
FS#show ipv6 policy
Banlance Mode: redundance
Interface                    Route map
VLAN 1                          RM_for_Vlan_1
VLAN 2                          RM_for_Vlan_2
```

Field	Description
Balance Mode	The current PBR running mode.
Interface	The name of interface with PBR applied.
Route map	The name of route map applied on the interface.

Related Commands

Command	Description
show route-map	Displays the current configured route map.

Platform Description

N/A

2 ROUTE-DB Commands

2.1 route-auto-choose

Use this command to configure a route database.

route-auto-choose { **cnc** | **cnii** | **cernet** | **cmcc** | **other** *word* } *interface next-hop* [**tag** *num*] [*distance*]

Use the **no** form of this command to delete a route database.

no route-auto-choose { **cnc** | **cnii** | **cernet** | **cmcc** | **other** *word* } *interface next-hop* [**tag** *num*] [*distance*]

Use this command to restore the default configuration.

default route-auto-choose { **cnc** | **cnii** | **cernet** | **cmcc** | **other** *word* } *interface next-hop* [**tag** *num*] [*distance*]

Parameter Description

Parameter	Description
cnc	Configure the China Unicom route database.
cnii	Configure the China Telecom route database.
cernet	Configure the route database of the education network.
cmcc	Configure the China Mobile route database.
word	Configure a route database of another operator type.
interface	Indicate the outbound routing interface corresponding to the route database.
next-hop	Indicate the next-hop IP address of the route corresponding to the route database.
tag *num*	Indicate the tag of the route corresponding to the route database.
distance	Indicate the metric value for a route of the route database.

Defaults

No route database is configured by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to associate a route database with a specified interface.

Configuration Example

#Configure a route database command to enable the China Telecom route database. The interface is gigabitEthernet 0/1 and the next-hop IP address is 202.100.12.5.

```
FS# config
FS(config)# route-auto-choose cnii gigabitEthernet 0/1 202.100.12.5
```

Verification

1. Run the **show route-db-info cnii** command to display information about the corresponding China Telecom route database.

2. Verify that corresponding information is prompted when the next-hop IP address of the route database is the local IP address.

```
FS(config)#route-auto-choose cmcc gi 0/5 192.168.55.111
```

```
%Invalid next hop address (it's this router)
```

2.2 route-auto-choose update

Use this command to update the route database file, and then update the currently running route database based on the updated route database file.

route-auto-choose update

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Global configuration mode

Usage Guide Use this command to update the route database.

Configuration Example

#Update the route database file.

```
FS# config
FS(config)# route-auto-choose update
```

2.3 route-auto-choose user-defined

Use this command to configure a user-defined route database.

route-auto-choose user-defined name *string* [*ip_address ip_mask*]

Use the **no** form of this command to delete a user-defined route database.

no route-auto-choose user-defined name *string* [*ip_address ip_mask*]

Parameter Description

Parameter	Description
string	Name of the user-defined route database.
ip-address	IP address of the user-defined route database.
ip_mask	Mask of the user-defined route database.
file-path	Import path

Default Settings There is no user-defined route database by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to associate a route database with a specified interface.

Configuration Example

1: Configure a user-defined route database. Its name is “Hello”, the IP address is 1.1.1.1, and the mask is 255.255.255.255.

```
FS# config

FS(config)# route-auto-choose user-defined Hello 1.1.1.1 255.255.255.255
```

Verification

Run the command **show route-db-info user-defined** to display information of the user-defined route database.

Prompt

1: If the name of the user-defined route database is the same as the name of the default route database, the configuration fails and the system shows the corresponding prompt.

```
FS(config)# route-auto-choose user-defined name cmcc

"cmcc" exists in default types, please rename!
```

2.4 show route-db-info

Use this command to display the route database information.

show route-db-info { **cnc** | **cnii** | **cernet** | **cmcc** | *word* | **db-type** | *ip_address* | **user-defined** }

Parameter Description

Parameter	Description
cnc	Check information about the China Unicom route database.
cnii	Check information about the China Telecom route database.
cernet	Check information about the route database of the education network.
cmcc	Check information about the China Mobile route database.
word	Check information about the route database of another operator type.
db-type	Check the number of operator types in the current route database file.
ip_address	Check the operator type of a certain IP address.
user-defined	Check the information about the user-defined route database.

Command Mode

All modes

Usage Guide

Use this command to query information about a route database.

Configuration Example

#Query all operator types in the route database

```
FS# show route-db-info db-type

cnii    China Telecom    2018.06.10.00

cnc    China Unicom    2018.06.10.00

cernet    Education    2018.06.10.00

cmcc    China Mobile    2018.06.10.00

beijingteletron    Beijing Teletron    2018.06.10.00

1 (User-defined)
```

Field	Description
The first column	English abbreviation of operator
The second column	Chinese name of operator
The third column	Version of operator’s route database
User-defined	Indicate this operator is a user-defined one

3 RIP Commands

3.1 auto-summary

Use this command to enable automatic summary of RIP routes. Use the **no** form of this command to disable this function

auto-summary

no auto-summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults Automatic summary of RIP routes is enabled by default

Command Mode Routing progress configuration mode

Usage Guide Automatic RIP route summary means the subnet routes will be automatically summarized into the routes of the classified network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2.

Automatic RIP route summary improves the flexibility and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the routing table, reducing the size of the routing table significantly.

Advertising the summarized route is more efficient than advertising individual routes in light of the following factors:

- The summarized route is always processed preferentially when you query the RIP database.
- Any sub-route is ignored when you query the RIP database, reducing the processing time.
- If you want to learn the specific sub-routes instead of the summarized route, disable the automatic route summary function. Only when RIPv2 is configured, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.

The range of the supernet route is wider than that of the classful network. Therefore, this command takes no effect on the supernet route.

Configuration Examples The following example disables automatic route summary of RIPv2.

```
FS (config)# router rip
FS (config-router)# version 2
FS (config-router)# no auto-summary
```

Related Commands

Command	Description
version	Defines the RIP software versions: v1 or v2. Both v1

	and v2 are supported by default.

Platform Description N/A

3.2 default-information originate

Use this command to generate a default route in the RIP progress. Use the **no** form of this command to delete the generated default route.

default-information originate [**always] [metric** *metric-value*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**route-map** *map-name*]

Parameter Description

Parameter	Description
always	(Optional) Enables RIP to generate the default route, no matter whether the default route exists or not.
metric *metric-value*	(Optional) The original metric value of the default route with the value range 115 of metric-value.
route-map *map-name*	(Optional) Name of the associated route-map. Route-map is not associated by default.

Defaults No default route is generated by default.

The default metric value is 1.

Command Mode Routing process configuration mode

Usage Guide By default, RIP will not advertise the default route if the default route exists in the routing table of the router. In this case, use the **default-information originate** command to notify the neighbor of the default route.

With the parameter always configured, no matter whether the default route exists in the RIP routing process or not, the default route will be advertised to the neighbor but is not shown in the local routing table. You can use the **show ip rip database** command to view the RIP routing information database to confirm whether the default route is generated.

Use the parameter **route-map** to control more about the default route advertised to RIP. For example, use the **set metric** command to set the metric value of the default route.

The route-map set metric rule takes precedence over the parameter metric value configuration of the default route. If the parameter metric is not configured, the default metric value is used by the default route.

ℹ If the default route can be generated in the RIP process by using this command, RIP will not learn the default route advertised from the neighbor.

ℹ For the default route generated by using the ip default-network command, the default-information originate command is required to add the default route to RIP.

Configuration The following example generates a default route to the RIP routing table.

Examples

```
FS(config-router)# default-information originate always
```

Related Commands

Command	Description
ip rip default-information	Notifies the default route through an interface.
redistribute	Redistributes the routes from other protocols to RIP.

Platform Description N/A

3.3 default-metric

Use this command to define the default RIP metric value. Use the **no** form of this command to restore the default setting.

default-metric *metric-value*

no default-metric

Parameter Description

Parameter	Description
metric-value	Indicates the default metric value with the range from 1 to 16. If the metric value is greater than or equal to 16, the FSNOS regards the route unreachable.

Defaults The default is 1.

Command Mode Routing process configuration mode

Usage Guide This command needs to work with the command **redistribute**. When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric value cannot be converted due to the incompatibility of the metric calculation mechanisms for different protocols. During the conversion, therefore, it is required to redefine the metric values of redistributed routes in the RIP routing domain. If there is no clear definition of the metric value in redistributing a routing protocol process, the RIP uses the metric value defined with **default-metric**. If the metric value is defined, this value overwrites the metric value defined with default-metric. If this command is not configured, the default value of default-metric is 1.

Configuration Examples The following example enables the RIP routing protocol to redistribute the routes learned by the OSPF routing protocol, whose initial RIP metric value is set to 3.

```
FS (config)# router rip
FS (config-router)# default-metric 3
FS (config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the routes from one routing domain to

	another routing domain.

Platform Description N/A

3.4 distance

Use this command to set the management distance of the RIP route. Use the **no** form of this command to restore the default setting.

distance *distance* [*ip-address wildcard*]

no distance [*distance ip-address wildcard*]

Parameter Description

Parameter	Description
distance	Sets the management distance of a RIP route, an integer in the range from 1 to 255.
ip-address	Indicates the prefix of the source IP address of the route.
wildcard	Defines the comparison bit of the IP address, where 0 means accurate matching and 1 means no comparison.

Defaults The default is 120.

Command Mode Routing process configuration mode

Usage Guide Use this command to set the management distance of the RIP route.

You can use this command to create several management distances with source address prefixes. When the source address of the RIP route is within the range specified by the prefixes, the corresponding management distance is applied; otherwise, the route uses the management distance configured by the RIP.

Configuration Examples The following example sets the management distance of the RIP route to 160, and specifies the management distance of the route learned from 192.168.2.1 as 123.

```
FS(config)# router rip
FS(config-router)# distance 160
FS(config-router)# distance 123 192.168.12.1 0.0.0.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.5 distribute-list in

Use this command to control route update for route filtering. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

Parameter Description

Parameter	Description
access-list-number | *name*	Specifies the ACL. Only the routes that are allowed by the ACL can be accepted.
prefix *prefix-list-name*	Uses the prefix list to filter the routes.
gateway *prefix-list-name*	Uses the prefix list to filter the source of the routes.
interface-type interface-number	(Optional) Applies the distribution list only to a specified interface.

Defaults

The distribution list is not defined by default.

Command Mode

Routing process configuration mode

Usage Guide

To deny receiving some specified routes, you can process all the received route update packets by configuring the route distribute control list.

Without any interface specified, the system will process the route update packets received on all the interfaces.

Configuration Examples

The following example enables RIP to control the routes received from the Fastethernet 0/0, only permitting the routes starting with 172.16.

```
FS (config)# router rip
FS (config-router)# network 200.168.23.0
FS (config-router)# distribute-list 10 in fastethernet 0/0
FS (config-router)# no auto-summary
FS (config-router)# access-list 10 permit 172.16.0.0 0.0.255.255
```

Related Commands

Command	Description
access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.

Platform Description

N/A

3.6 distribute-list out

Use this command to control route update advertisement for filtering routes. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-nam*e } **out** [*interface* **|** [**connected | ospf** *process-id* **| rip | static**]]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-nam*e } **out** [*interface* **|** [**connected | ospf** *process-id* **| rip | static**]]

Parameter Description

Parameter	Description
access-list-number | *name*	Specifies the ACL.
prefix *prefix-list-name*	Uses the prefix list to filter routes.
interface	(Optional) Applies route update advertisement control to a specified interface in the distribution list.
connected	(Optional) Applies route update advertisement control to only connected routes in this distribution list.
ospf *process-id*	(Optional) Applies route update advertisement control to only routes introduced from OSPF in this distribution list. *process-id* specifies an OSPF instance.
rip	(Optional) Applies route update advertisement control to only RIP routes in this distribution list.
static	(Optional) Applies route update advertisement control to only static routes in this distribution list.

Defaults No route update advertisement is configured by default.

Command Mode Routing process configuration mode

Usage Guide If this command relates to none of optional parameters, route update advertisement control applies to all interfaces. If this command relates to interface options, route update advertisement control applies to only the specified interface. If this command relates to other route process parameters, route update advertisement control applies to only the specific route process.

Configuration Examples The following example advertises only the 192.168.12.0/24 route.

```
FS (config)# router rip
FS (config-router)# network 200.4.4.0
FS (config-router)# network 192.168.12.0
FS (config-router)# distribute-list 10 out
FS (config-router)# version 2
FS (config-router)#access-list 10 permit 192.168.12.0 0.0.0.255
```

Related

Command	Description

Commands

access-list	Defines the ACL rule.
prefix-list	Defines the prefix list.
redistribute	Configures route redistribution.

Platform Description N/A

3.7 enable mib-binding

Use this command to bind a MIB with a specified RIP instance. Use the **no** form of this command to restore the default setting

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command Mode Routing process configuration mode.

Usage Guide

Configuration Examples

Related Commands

Command	Description
show ip rip	Displays the global configuration of RIP.

Platform Description N/A

3.8 graceful-restart

Use this command to configure the RIP graceful restart (GR) function for a device. Use the **no** form of this command to restore the default configuration.

graceful-restart [**grace-period** *grace-period*]

no graceful-restart [**grace-period**]

Parameter Description

Parameter	Description

graceful-restart	Enables the GR function.
grace-period	(Optional) Configures the grace period.
grace-period	(Optional) Indicates the user-defined GR period. The default value is the smaller value between twice the update time and 60 seconds. The range is from 1 to 1,800. The unit is second.

Defaults

This function is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

The GR function is configured on the RIP instances. Different parameters can be configured for different RIP instances.

The GR period refers to the time from the startup to the end of RIP GR. During this period, the forwarding table remains unchanged and the RIP route is restored to the state before protocol restart. When the GR period expires, RIP exits the GR state and performs normal RIP operation.

The **graceful-restart grace-period** command enables users to modify GR period. Note: Make sure that GR is completed before the RIP route is validate and after an RIP route update cycle elapses. If an improper value is configured, non-stop data forwarding cannot be ensured during the GR process. For example, if the GR period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not re-informed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the period needs to changed, determine that the grace period is longer than the route update cycle and shorter than the time when the route is unavailable in combination with the configuration of the **timers basic** command.

⚠ During the RIP GR period, the network must be stable.

Configuration Examples

The following example enables the RIP GR function and configures the GR period parameters of the GR function.

```
FS(config)# router rip
FS(config-router)# graceful-restart grace-period 90
```

Related Commands

Command	Description
timers basic	Configures RIP timers.

Platform Description

N/A

3.9 ip rip authentication key-chain

Use this command to enable RIP authentication and specify the keychain used for RIP authentication. Use the **no** form of this command to restore the default setting.

ip rip authentication key-chain *name-of-keychain*

no ip rip authentication key-chain

Parameter Description

Parameter	Description
name-of-keychain	Indicates the name of the keychain, which specifies the keychain used for RIP authentication.

Defaults The keychain is not associated by default.

Command Mode Interface configuration mode

Usage Guide If the keychain is specified in the interface configuration, use the key chain global configuration command to define the keychain. Otherwise, RIP data packet authentication fails.

RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples The following example enables RIP authentication on the fastEthernet 0/1 with the associated keychain ripchain.

```
FS (config)#interface fastEthernet 0/1
FS (config-if-FastEthernet 0/1)#ip rip authentication key-chain ripchain
```

Meanwhile, use the **key chain** command to define this keychain in global configuration mode.

```
FS(config)#key chain ripchain
FS(config-keychain)#key 1
FS(config-keychain-key)#key-string Hello
```

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication text-password	Enables RIP authentication, and sets the password string of RIP plaintext authentication. RIP data packet authentication is supported only by RIPv2.
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
key chain	Defines the keychain and enters keychain configuration mode.

Platform Description N/A

3.10 ip rip authentication mode

Use this command to define the RIP authentication mode. Use the **no** form of this command to restore the default setting.

ip rip authentication mode { **text | md5** }

no ip rip authentication mode

Parameter Description

Parameter	**Description**
text	Configures RIP authentication as plaintext authentication.
md5	Configures RIP authentication as MD5 authentication.

Defaults It is plaintext authentication by default.

Command Mode Interface configuration mode

Usage Guide During the RIP authentication configuration process, the RIP authentication modes of all devices requiring exchange of RIP routing information must be the same. Otherwise, RIP packet exchange will fail.

If the plaintext authentication mode is adopted, but the password string of the plaintext authentication or the associated keychain is not configured, no authentication occurs. In the same way, if the MD5 authentication mode is adopted, but the associated keychain is not configured, no authentication occurs.

RIPv2 instead of RIPv1 supports authentication of the RIP data packet.

Configuration Examples The following example configures the RIP authentication mode on the fastEthernet 0/1 as MD5.

```
FS (config)#interface fastEthernet 0/1
FS (config-if-FastEthernet 0/1)# ip rip authentication mode md5
```

Related Commands

Command	**Description**
ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication of the RIP data packet.
ip rip authentication text-password	Enables the RIP authentication mode, and sets the password string of RIP plaintext authentication. Only RIPv2 supports authentication of the RIP data packet.
key chain	Defines the keychain and enters the keychain configuration mode

Platform Description N/A

3.11 ip rip authentication text-password

Use this command to enable RIP authentication and set the password string of RIP plaintext authentication. Use the **no** form of this command to restore the default setting.

ip rip authentication text-password [**0** | **7**] *password-string*

no ip rip authentication text-password

Parameter Description

Parameter	Description
0	Specifies that the key is displayed as plaintext.
7	Specifies that the key is displayed as cipher text.
password-string	Indicates the password string of the plaintext authentication, in the length of 1-16 bytes.

Defaults

No password string of RIP plaintext authentication is configured by default.

Command Mode

Interface configuration mode

Usage Guide

This command works only in plaintext authentication mode.

To enable the RIP plaintext authentication function, use this command to configure the corresponding password string, or use the associated key chain to obtain the password string. The latter takes the precedence over the former one.

RIPv1 does not support RIP authentication but RIPv2 does.

Configuration Examples

The following example enables the RIP plaintext authentication on fastEthernet 0/1 and sets the password string to hello.

```
FS(config)#interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip rip authentication text-password hello
```

Related Commands

Command	Description
ip rip authentication mode	Defines the RIP authentication mode.
ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication.

Platform Description

N/A

3.12 ip rip default-information

Use this command to advertise the default route through a RIP interface. Use the **no** form of this command to restore the default setting.

ip rip default-information { **only** | **originate** } [**metric** *metric-value*]

no ip rip default-information

Parameter Description

Parameter	Description

only	Notifies the default route rather than other routes.
originate	Notifies the default route and other routes.
metric *metric-value*	Specifies the metric value of the default route, in the range from1 to 15.

Defaults No default route is configured by default. The default metric value is 1.

Command Mode Interface configuration mode

Usage Guide After you configure this command on a specified interface, a default route is generated and notified through the interface. If the **ip rip default-information** command of the interface and the **default-information originate** command of the RIP process are configured at the same time, only the default route of the interface is advertised.

RIP will no longer learn the default route notified by the neighbor if any interface is configured with the ip rip default-information command.

Configuration Examples The following example creates a default route which is notified on ethernet0/1 only.

```
FS(config)#interface ethernet 0/1
FS(config-if-Ethernet 0/1)#ip rip default-information only
```

Related Commands

Command	Description
default-information originate	Generates a default route in the RIP process.

Platform Description N/A

3.13 ip rip receive enable

Use this command to enable RIP to receive the RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

ip rip receive enable

no ip rip receive enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RIP packages can be received through the interface by default.

Command Mode Interface configuration mode

Usage Guide

To prevent an interface from receiving RIP packets, use the no form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to receive the RIP data package.

Configuration Examples

The following example prohibits receiving RIP data packages on fastEthernet 0/1.

```
FS (config)# interface fastEthernet 0/1
FS (config-if-FastEthernet 0/1)# no ip rip receive enable
```

Related Commands

Command	Description
ip rip send enable	Enables or disables the interface to send RIP data packages.
passive-interface	Configures a passive RIP interface.

Platform Description

N/A

3.14 ip rip receive version

Use this command to define the version of RIP packets received on an interface. Use the **no** form of this command to restore the default setting.

ip rip receive version [**1**] [**2**]

no ip rip receive version

Parameter Description

Parameter	Description
1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults

The default behavior depends on the configuration with the version command.

Command Mode

Interface configuration mode

Usage Guide

This command overwrites the default configuration of the **version** command. It affects only RIP packet receiving through the interface and allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If the command is configured without parameters, data package receiving depends on the configuration of the version.

Configuration Examples

The following example enables receiving both RIPv1 and RIPv2 data packages.

```
FS (config)#interface fastEthernet 0/1
FS (config-if-FastEthernet 0/1)# ip rip receive version 1 2
```

Related Commands

Command	Description

version	Defines the default version of the RIP packets received/sent on the interface.

Platform Description N/A

3.15 ip rip send enable

Use this command to enable RIP to send a RIP data package on a specified interface. Use the **no** form of this command to restore the default setting.

ip rip send enable

no ip rip send enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults RIP packages can be sent through the interface by default.

Command Mode Interface configuration mode

Usage Guide To prevent an interface from sending RIP packets, use the **no** form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the **default** form of this command to enable the interface to send the RIP data package.

Configuration Examples The following example prohibits sending RIP data packages on fastEthernet 0/1.

```
FS (config)# interface fastEthernet 0/1
FS (config-if-FastEthernet 0/1)# no ip rip send enable
```

Related Commands

Command	Description
ip rip receive enable	Enables or disables receiving RIP packets on the interface.
passive-interface	Configures a passive RIP interface.

Platform Description N/A

3.16 ip rip send supernet-routes

Use this command to enable RIP to send the supernet route on a specified interface. Use the **no** form of this command to disable this function.

ip rip send supernet-routes

no ip rip send supernet-routes

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Interface configuration mode

Usage Guide When the RIPv1 router monitors a RIPv2 router response packet and if the supernet routing information is monitored, incorrect route information is learned because the RIPv1 ignores the subnet mask of the routing information. In this case, you are advised to use the no form of this command on the RIPv2 router to disable advertising the supernet route on the corresponding interface. This command works only on interfaces configured with this command.

ℹ This command is only valid upon sending the RIPv2 packets on the interface and it is used to control sending the supernet route.

Configuration Examples The following example disables sending RIP supernet routes on the fastEthernet 0/1 interface.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# no ip rip send supernet-routes
```

Related Commands

Command	Description
version	Defines the RIP version
ip rip send enable	Enables or disables sending the RIP package on the interface.

Platform Description N/A

3.17 ip rip send version

Use this command to define the version of the RIP packets sent on the interface. Use the **no** form of this command to restore the default setting.

ip rip send version [**1**] [**2**]

no ip rip send version

Parameter Description

Parameter	Description
1	(Optional) Receives only RIPv1 packets.
2	(Optional) Receives only RIPv2 packets.

Defaults

The default behavior depends on the configuration with the version command.

Command Mode

Interface configuration mode

Usage Guide

This command overwrites the default configuration of the **version** command. It affects only RIP packet sending through the interface and allows RIPv1 and RIPv2 packages sent on the interface at the same time. If the command is configured without parameters, package receiving depends on the configuration of the version.

Configuration Examples

The following example enables sending both RIPv1 and RIPv2 packages on the fastEthernet 0/1 interface.

```
FS (config)# interface fastEthernet 0/1
FS (config-if-FastEthernet 0/1)# ip rip send version 1 2
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received/sent on the interfaces.

Platform Description

N/A

3.18 ip rip split-horizon

Use this command to enable split horizon. Use the **no** form of this command to disable this function.

ip rip split-horizon [**poisoned-reverse**]

no ip rip split-horizon [**poisoned-reverse**]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables split horizon with poisoned reverse.

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode

Usage Guide

When multiple devices are connected to the IP broadcast network and run a distance vector routing protocol, the split horizon mechanism is required to prevent loop. The split horizon prevents the device from advertising routing information from the interface that learns that information, which optimizes routing information exchange between multiple devices.

For non-broadcast multi-path access networks (such as frame relay and X.25), split horizon may cause some devices to be unable to learn all routing information. Split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for split horizon.

If the **poisoned-reverse** parameter is configured, split horizon with poisoned reverse is enabled. In this case, devices still advertise the route information through the interface from which the route information is learned. However, the metric value of the route information is set to unreachable.

The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, use the show ip rip command to judge. This function makes no influence on the neighbor defined with the **neighbor** command.

Configuration Examples

The following example disables the RIP split horizon function on the interface fastethernet 0/0.

```
FS (config)# interface fastethernet 0/1
FS (config-if)# no ip rip split-horizon
```

Related Commands

Command	Description
neighbor (RIP)	Defines the IP address of the neighbor of RIP.
validate-update-source	Enables the source address authentication of the RIP route update message.

Platform Description

N/A

3.19 ip rip summary-address

Use this command to configure port-level convergence through an interface. Use the **no** form of this command to disable this function.

ip rip summary-address *ip-address ip-network-mask*

no ip rip summary-address *ip-address ip-network-mask*

Parameter Description

Parameter	Description
ip-address	Indicates the IP addresses to be converged.
ip-network-mask	Indicates the subnet mask of the specified IP address for route convergence.

Defaults

The RIP routes are automatically converged to the classful network edge by default.

Command Mode

Interface configuration mode

Usage Guide

The **ip rip summary-address** command converges an IP address or a subnet on a specified port. RIP routes are automatically converged to the classful network edge. The classful subnet can be configured through only port convergence.

The summary range configured by this command cannot be a super class network, that is, the configured mask length is greater than or equal to the natural mask length of the network.

Configuration

The following example disables the automatic route convergence function of RIPv2. Interface convergence is

Examples

configured so that fastEthernet 0/1 advertises the converged route 172.16.0.0/16.

```
FS (config)# interface fastEthernet 0/1
FS (config-if-FastEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0
FS (config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
FS (config)# router rip
FS (config-router)# network 172.16.0.0
FS (config-router)# version 2
FS (config-router)# no auto-summary
```

Related Commands

Command	Description
auto-summary	Enables the automatic convergence of RIP routes.

Platform Description

N/A

3.20 ip rip triggered

Use this command to enable triggered RIP based on links. Use the **no** form of this command to restore the default setting.

ip rip triggered

ip rip triggered retransmit-timer *timer*

ip rip triggered retransmit-count *count*

no ip rip triggered

no ip rip triggered retransmit-timer

no ip rip triggered retransmit-count

Parameter Description

Parameter	Description
retransmit-timer *timer*	Configures the interval at which the Update Request and Update Response packets are retransmitted. The range is from 1 to 3,600. The unit is second. The default is five.
retransmit-count *count*	Configures the maximum times that the Update Request and Update Response packets are retransmitted. The range is from 1 to 3600. The default is 36.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Triggered RIP (TRIP) is the extension of RIP on the wide area network (WAN), mainly used for demand-based links. With the TRIP function enabled, RIP no longer sends route updates periodically and sends route updates to the WAN interface only if:

Update Request packets are received.

RIP routing information is changed.

Interface state is changed.

The router is started.

As periodical RIP update is disabled, the confirmation and retransmission mechanism is required to ensure that update packets are sent and received successfully over the WAN. The **retransmit-timer** and **retransmit-count** commands can be used to specify the retransmission interval and maximum retransmission times for request and update packets.

⚠ The function can be enabled in the case of the following conditions: a) The interface has only one neighbor. b) There are multiple neighbors but they interact information using unicast packets. You are advised to enable the function for link layer protocols such as PPP, frame relay, and X.25.

⚠ You are advised to enable split horizon with poison reverse on the interface enabled with the function; otherwise invalid routing information might be left.

⚠ Make sure that the function is enabled on all routers on the same link; otherwise the function will be invalid and the routing information cannot be exchanged correctly.

⚠ To enable the function, make sure that the RIP configuration is the same on both ends of the link, such as RIP authentication and the RIP version supported by the interface.

⚠ If this function is enabled on this interface, the source address of packets on this interface will be checked no matter whether the source IP address verification function (validate-update-source) is enabled.

Configuration Examples

The following example enables TRIP and sets the retransmission interval and maximum retransmission time to 10 seconds and 18 respectively for Update Request and Update Response packets.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip rip triggered
FS(config-if-FastEthernet 0/1)# ip rip triggered retransmit-timer 10
FS(config-if-FastEthernet 0/1)# ip rip triggered retransmit-count 18
```

Related Commands

Command	Description
show ip rip database	Displays the summarized routing information of the RIP database.
show ip rip interface	Displays the RIP interface information.
ip rip split-horizon	Configures RIP split horizon.

Platform Description

N/A

3.21 ip rip v2-broadcast

Use this command to send RIPv2 packets in broadcast rather than multicast mode. Use the **no** form of this command to restore the default setting.

ip rip v2-broadcast

no ip rip v2-broadcast

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default behavior depends on the configuration of the version command.

Command Mode Interface configuration mode

Usage Guide This command overwrites the default of the **version** command. This command affects only sending RIP packets on the interface. This command allows RIPv1 and RIPv2 packages sent on the interface simultaneously. If this command is configured without parameters, package receiving depends on the version setting.

Configuration Examples The following example sends RIPv2 packets in broadcast mode on the fastEthernet 0/1 interface.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# no ip rip split-horizon
```

Related Commands

Command	Description
version	Defines the default version of the RIP packets received and sent on the interface.

Platform Description N/A

3.22 neighbor

Use this command to define the IP address of a RIP neighbor. Use the **no** form of this command to restore the default setting.

neighbor *ip-address*

no neighbor *ip-address*

Parameter Description

Parameter	Description
ip-address	Indicates the IP address of the neighbor. The IP address must be that of the network connected to the local device.

Defaults The neighbor is not defined by default.

Command Mode Routing process configuration mode

Usage Guide

By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 uses the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, use the **passive-interface** command to configure related interfaces as passive interfaces and then define only some neighbors who can receive the routing information. This command has no impact on the receiving of RIP information. The passive interface is configured. No request packet is sent after the interface is enabled.

Configuration Examples

The following example creates a VRF with the name of vpn1 and creates its RIP instance.

```
FS(config)# ip vrf vpn1
FS(config-vrf)# exit
FS(config)# interface fastEthernet 1/0
FS(config-if-FastEthernet 0/1)# ip vrf forwarding vpn1
FS(config-if-FastEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
FS(config)# router rip
FS(config-router)# address-family ipv4 vrf vpn1
FS(config-router)# network 192.168.1.0
FS(config-router)# exit-address-family
```

Related Commands

Command	Description
passive-interface	Configures the interface as a passive interface.

Platform Description

N/A

3.23 network

Use this command to define the list of networks to be advertised in the RIP routing process. Use the **no** form of this command to delete the defined network.

network *network-number* [*wildcard*]

no network *network-number* [*wildcard*]

Parameter Description

Parameter	Description
network-number	Indicates the network number of the directly-connected network. The network number is a natural one. All interfaces whose IP addresses belong to that natural network can send/receive RIP packages.
wildcard	Defines the IP address comparing bit: 0 refers to accurate matching, and 1 refers to no comparison.

Defaults

N/A

Command

Routing process configuration mode

Mode

Usage Guide The *network-number* and *wildcard* parameters can be configured simultaneously to enable the IP address of the interface within the IP address range to join RIP running.

Without the *wildcard* parameter, FSOS make the interface IP address within the classful address range join the RIP running.

Only when the IP address of an interface is in the network list defined by RIP, RIP route update packets can be received and sent on the interface.

Configuration Examples The following example defines two network numbers associated with RIP and allows the interface IP address between 192.168.12.0/24 and 172.16.0.0/24 to join RIP running.

```
FS (config)# router rip
FS (config-router)# network 192.168.12.0
FS(config-router)# network 172.16.0.0 0.0.0.255
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.24 offset-list

Use this command to increase the metric value of received or sent RIP routes. Use the **no** form of this command to restore the default setting.

offset-list { access-list-number | name } { **in** | **out** } offset [interface-type interface-number]

no offset-list { access-list-number | name { **in** | **out** } offset [interface-type interface-number]

Parameter Description

Parameter	Description
access-list-number | name	Specifies the ACL.
in	Modifies the metric of the received routes using the ACL.
out	Modifies the metric of the sent routes using the ACL.
offset	Indicates the offset of changed metric values. The value is in the range from 0 to16.
interface-type	Applies the ACL to a specified interface.
interface-number	Specifies the interface number.

Defaults No offset is specified by default.

Command Mode Routing process configuration mode

Usage Guide

If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.

Configuration Examples

The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7.

```
FS (config-router)# offset-list 7 out 7
```

The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by fastethernet 0/1.

```
FS (config-router)# offset-list 8 in 7 fastethernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.25 output-delay

Use this command to modify the delay to send RIP update packets. Use the **no** form of this command to restore the default setting.

output-delay *delay*

no output-delay

Parameter Description

Parameter	Description
delay	Sets the delay to send RIP update packets, in the range from 8 to 50 in the unit of milliseconds.

Defaults

No sending delay is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

In normal cases, the size of a RIP update packet is 512 bytes including 25 routes. If the number of updated routes is greater than 25, update packets will be sent through multiple routes. Note that the update packets should be sent as fast as possible.

However, when a high-speed device sends a large number of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.

Configuration Examples

The following example sets the delay to send RIP update packets to 30 milliseconds.

```
FS(config)# router rip
FS(config-router)# output-delay 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.26 passive-interface

Use this command to disable the function of sending update packets on an interface. Use the **no** form of this command to restore the default setting.

passive-interface { **default |** *interface-type interface-num* }

no passive-interface { **default |** *interface-type interface-num* }

Parameter Description

Parameter	Description
default	Sets all interfaces to the passive interfaces.
interface-type interface-num	Indicates the interface type and number.

Defaults

Interfaces are set to the non passive interfaces by default.

Command Mode

Routing process configuration mode

Usage Guide

The **passive-interface default** command sets all interfaces to the passive interfaces. You can use **no passive-interface** *interface-type interface-num* command to set specified interfaces as non-passive interfaces. After you set an interface to the passive interface, RIP route update packets will no longer be sent but can be received through the interface. In this case, route update packets can be sent to a specified neighbor through the interfaces by using the **neighbor** command. You can use the **ip rip send enable** and **ip rip receive enable** commands to control whether route update packets can be sent or received through the interface.

Configuration Examples

The following example sets all interfaces to the passive interfaces and then sets ethernet0/1 to the non-passive interface.

```
FS(config-router)# passive-interface default
FS(config-router)# no passive-interface gigabitEthernet 0/1
```

Related Commands

Command	Description
ip rip receive enable	Enables or disables receiving RIP packets on the interface.
ip rip send enable	Enables or disables sending RIP packets on the interface.

Platform Description N/A

3.27 redistribute

Use this command to redistribute external routes in route configuration mode. Use the **no** form of this command to restore the default setting.

redistribute { **connected** | **ospf** *process-id* | **static** } [**match** { **internal | external** [**1 | 2**] **| nssa-external** [**1 | 2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]

no 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

Parameter	Description
connected	Is redistributed from a connected route.
ospf *process-id*	Is redistributed from OSPF and specifies an OSPF instance through process-id. The value is in the range from 1 to 65535.
static	Is redistributed from static routes.
match	Is used when OSPF route redistribution is configured and filters a route with a specific level for redistribution.
metric *metric-value*	Sets the metric value of the redistributed route and specifies the metric value by using the metric-value parameter. The value is in the range from 1 to 16.
route-map *route-map-name*	Sets the redistribution filtering rule.

Defaults

By default:

All the routes of the sub types of the instance are redistributed when you configure redistributing OSPF.

All the routes of the protocol are redistributed for other routing protocols.

The metric of the redistributed routes is 1 by default.

The route-map is not associated.

Command Mode

Routing process configuration mode

Usage Guide

This command is executed to redistribute external routes to RIP.

It is unnecessary to convert the metric of one routing protocol into that of another routing protocol for route redistribution, since different routing protocols use different metric measurement methods. For RIP, the metric value is calculated based on hop counts; for OSPF, the metric value is calculated based on bandwidths. Therefore, their metrics are not comparable. However, a symbolic metric value must be set for route redistribution. Otherwise, route redistribution will fail.

When you configure redistribution of OSPF routes without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The no form of this command restores the setting to the default value.

The rule of configuring the no form of the redistribute command is as follows:

1. If the no form of this command specifies certain parameters, the parameters must be restored to the default configuration.

2. If the **no** form of this command does not specify any parameter, the command must be deleted.

Assume that the following configurations are available.

⚠ The redistribute command cannot redistribute the default route of other protocol to the RIP process. To this end, use the **default-information originate** command.

Configuration Examples

The following example redistributes static routes to RIP.

```
FS(config-router)# redistribute static
```

Related Commands

Command	Description
default-metric *metric*	Sets the default metric of the route to be redistributed.
default-information originate	Generates the default route in the RIP process.

Platform Description

N/A

3.28 router rip

Use this command to create the RIP routing process and enter the routing process configuration mode. Use the **no** form of this command to restore the default setting.

router rip

no router rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No RIP process is running by default.

Command Mode

Global configuration mode

Usage Guide

One RIP routing process must be defined with one network number. If a dynamic routing protocol runs on asynchronous lines, configure the **async default routing** command on the asynchronous interface.

Configuration Examples

The following example creates the RIP routing process and enters the routing process configuration mode.

```
FS (config)# router rip
FS(config-router)#
```

Related Commands

Command	Description
network (RIP)	Defines the network number of the RIP process.

Platform Description

N/A

3.29 show ip rip

Use this command to display the RIP process information.

show ip rip

Parameter Description

Parameter	Description

Defaults

N/A

Command Mode

Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide

It is used to display the three timers, routing distribution status, routing re-distribution status, interface RIP version, RIP interface and network range, metric, and distance of the RIP process quickly.

Configuration Examples

The following example displays the basic information of the RIP process such as the update time and management distance.

```
FS#show ip rip
Routing Protocol is "rip"
  Sending updates every 10 seconds, next due in 4 seconds
  Invalid after 20 seconds, flushed after 10 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 2
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface                Send   Recv
    FastEthernet 0/1          2      2
    FastEthernet 0/2          2      2
  Routing for Networks:
    192.168.26.0 255.255.255.0
    192.168.64.0 255.255.255.0
  Distance: (default is 50)
Graceful-restart enabled
  Restart grace period 60 secs
```

```
Current Restart remaining time 16 secs
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.30 show ip rip database

Use this command to display the route summary information in the RIP routing database.

show ip rip database [*network-number network-mask*] [**count**]

Parameter Description

Parameter	Description
network-number	(Optional) Indicates the ID of the subnet on which route information is to be displayed.
network-mask	Indicates the subnet mask. It must be specified if the network number is specified.
count	(Optional) Displays the abstract of the route statistics in the RIP database.

Defaults

N/A

Command Mode

Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide

Only when the related sub-routes are converged, the converged address entries appear in the RIP routing database. When the last sub-route information in the converged address entries becomes invalid, the converged address information will be deleted from the database.

Configuration Examples

The following example displays all converged address entries in the RIP routing database.

```
FS# show ip rip database
192.168.1.0/24      auto-summary
192.168.1.0/30      directly connected, Loopback 3
192.168.1.8/30      directly connected, FastEthernet 0/1
192.168.121.0/24      auto-summary
192.168.121.0/24      redistributed
[1] via 192.168.2.22, FastEthernet 0/2
192.168.122.0/24      auto-summary
192.168.122.0/24
[1] via 192.168.4.22, Serial 0/1    00:28      permanent
```

The following example displays the converged address entries related with 192.168.121.0/24 in the RIP routing database.

```
FS# show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24        redistributed
[1] via 192.168.2.22, FastEthernet 0/1
```

The following example displays the statistical information summary of various routes in the RIP routing database.

```
FS# show ip rip database count
                    All       Valid     Invalid
database           5          5          0
auto-summary       5          5          0

connected          1          1          0
rip                4          4          0
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently-running routing protocol process.

Platform Description N/A

3.31 show ip rip external

Use this command to display the information of the external routes redistributed by the RIP protocol.

show ip rip external [**connected** | **ospf** *process-id* | **static**]

Parameter Description

Parameter	Description
connected	Displays redistributed directly connected routes.
ospf ***process-id***	Displays redistributed OSPF routes. The process-id parameter indicates OSPF process ID. The range is from 1 to 65535.
static	Displays redistributed static routes.

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide N/A

Configuration Examples The following example displays direct routes redistributed by the RIP process.

```
FS# show ip rip external
Protocol connected route:
```

```
[connected] 192.100.3.0/24 metric=0
         nhop=0.0.0.0, if=2
  [connected] 192.101.1.0/24 metric=0
         nhop=0.0.0.0, if=3
Protocol static route:
  [static] 10.1.1.1/32 metric=0
         nhop=0.0.0.0, if=4096
  [static] 10.1.2.1/32 metric=0
         nhop=0.0.0.0, if=4096
Protocol ospf 1 route:
  [ospf] 1.1.1.1/32 metric=2
         nhop=192.100.3.2, if=2
  [ospf] 90.1.1.1/32 metric=2
         nhop=192.100.3.2, if=2
```

Related Commands

Command	**Description**
show ip rip	Displays the information of the currently running routing protocol process.
ip vrf	Creates a VRF.

Platform Description N/A

3.32 show ip rip interface

Use this command to display the RIP interface information.

show ip rip interface [interface-type interface-number]

Parameter Description

Parameter	**Description**
[*interface-type interface-number*]	Displays the specified interface type and interface number (optional).

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide This command is used to display the information about RIP interfaces. If no RIP interface exists, no information is displayed.

Configuration Examples The following example displays the RIP interface information.

```
FS# show ip rip interface
```

```
FastEthernet 0/1 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv2 packets only
Send RIPv2 packets only
Recv RIP packet total: 0
Send RIP packet total: 3
Passive interface: Disabled
Split Horizon with Poisoned Reverse: Enabled
Triggered RIP Enabled:
Retransmit-timer: 5, Retransmit-count: 36
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:
Not Configured
Authentication mode: Text
Authentication key-chain: ripk1
Authentication text-password: FS
Default-information: only, metric 5
IP interface address:
192.168.64.100/24, next update due in 14 seconds
2.2.1.1/24, next update due in 24 seconds
    neighbor 2.2.1.6, next update due in 3 seconds
    neighbor 2.2.1.77, next update due in 13 seconds
2.2.2.57/24, next update due in 16 seconds
```

Related Commands

Command	Description
show ip rip	Displays the information of the currently running routing protocol process.

Platform Description

N/A

3.33 show ip rip peer

Use this command to show the RIP peer information. RIP records a summary for the RIP routing information source learnt (source addresses of RIP route update packets) for the convenience of user monitoring. This routing information source is called RIP neighbor information.

show ip rip peer [*ip-address*]

Parameter Description

Parameter	Description
ip-address	(Optional) Displays the IP address of a specified RIP neighbor.

Defaults N/A

Command Mode Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode

Usage Guide This command is used to display the RIP neighbor information. If no RIP neighbor exists, no information will be displayed.

Configuration Examples The following example displays the RIP neighbor information.

```
FS# show ip rip peer
Peer 192.168.3.2:
    Local address: 192.168.3.1
    Input interface: GigabitEthernet 0/2
    Peer version: RIPv1
    Received bad packets: 3
    Received bad routes: 0
    BFD session state up
```

Related Commands

Command	Description
show ip rip	Displays the information of the routing protocol process that is running.

Platform Description N/A

3.34 timers basic

Use this command to adjust the RIP clock. Use the **no** form of this command to restore the default setting.

timers basic *update invalid flush*

no timers basic

Parameter Description

Parameter	Description
update	Indicates the route update time in seconds. The update keyword defines the period at which the device sends route update packets. Each time an update packet is received, the "Invalid" and "Flush" clocks are reset. By default, a route update packet is sent every 30 seconds.
invalid	Indicates the route invalid time in seconds, starting from the last valid update packet. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update packet is received within the route invalid period, the related route becomes invalid and enters into the "invalid" state. If an update packet is received within the period, the clock

	resets. By default, the Invalid time is 180 seconds.
flush	Indicates the route flushing time in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush time is 120 seconds.

Defaults

By default, the update time is 30 seconds, the invalid time is 180 seconds, and the flushing time is 120 seconds.

Command Mode

Routing process configuration mode

Usage Guide

Adjusting the above clocks may speed up routing protocol convergence and fault recovery. Devices connected to the same network must have consistent RIP clock values. Adjustment of RIP clocks is not recommended unless otherwise specified.

To check the current RIP clock parameters, use the **show ip rip** command.

⚠ If you set the clock to a small value on low-speed links, some risks will be caused because numerous update packets may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2 Mbit/s to reduce the convergence time of routes.

Configuration Examples

The following example enables the RIP update packets that are sent every 10 seconds. If no update packet is received within 30 seconds, related routes become invalid and enter the invalid status. When another 90s elapses, they will be cleared.

```
FS (config)# router rip
FS (config-router)# timers basic 10 30 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.35 validate-update-source

Use this command to validate the source address of the received RIP route update packet. Use the **no** form of the command to disable this function.

validate-update-source

no validate-update-source

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide You can validate the source address of the RIP route update packet. The validation aims to ensure that the RIP routing process receives only the route update packets from the same IP subnet neighbor.

Disabling split horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the **validate-update-source** command in routing process configuration mode.

In addition, for the ip unnumbered interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the command **validate-update-source**.

Configuration Examples The following example disables verification of the source IP address of the update packet.

```
FS (config)# router rip
FS (config-router)# no validate-update-source
```

Related Commands

Command	Description
ip split-horizon	Enables split horizon.
ip unnumbered	Defines the IP unnumbered interface.
neighbor (RIP)	Defines the IP address of a RIP neighbor.

Platform Description N/A

3.36 version

Use this command to define the RIP version of a device. Use the **no** form of this command to restore the default setting.

version { **1** | **2** }

no version

Parameter Description

Parameter	Description
1	Defines the RIP version 1.
2	Defines the RIP version 2.

Defaults The route update packets of RIPv1 and are received by default, but only the RIPv1 route update packets are sent.

Command Mode Routing process configuration mode

Usage Guide This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the **ip rip receive version** and **ip rip send version** commands.

Configuration Examples

The following example configures the RIP version as version 2.

```
FS (config)# router rip
FS (config-router)# version 2
```

Related Commands

Command	Description
ip rip receive version	Defines the version of RIP packets received on the interface.
ip rip send version	Defines the version of RIP packets sent on the interface.
show ip rip	Displays RIP information.

Platform Description

N/A

4 RIPng

4.1 clear ipv6 rip

Use this command to clear the RIPng routes.

clear ipv6 rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults

None

Command mode

Privileged EXEC mode

Usage Guide

Running this command removes all RIPng routes and this operation may have great impact on the RIPng protocol. This command should be used with caution.

Configuration Examples

The following example clears the RIPng routes:

```
FS# clear ipv6 rip
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.2 default-metric

Use this command to configure the default metric for RIPng. Use the **no** form of this command to restore the default value.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
metric	Sets the default metric value. The valid range is from 1 to 16. The route is unreachable if the metric value is larger than or equal to 16.

Defaults

The default value is 1.

Command mode

Routing process configuration mode.

Usage Guide

This command shall be used with the **redistribute** command. When redistributing the route from one route process to RIPng, due to the incompatibility of metric calculation mechanisms of different routing protocols, it fails to translate the routing metric values. To this end, the RIPng metric value shall be defined when translating the metric values. If there is no defined metric value, use the **default-metric** command to define one; and the defined metric value will overwrite the value of the **default-metric** command. By default, the **default-metric** value is 1.

Configuration Examples

The following example shows how to set the RIPng metric value as 3 when redistributing OSPF process 100:

```
FS(config-router)# default-metric 3
FS(config-router)# redistribute ospf 100
```

Related Commands

Command	Description
redistribute	Redistributes the route from one route domain to another route domain.

Platform Description

N/A

4.3 distance

Use this command to set the administrative distance of RIPng. Use the **no** form of this command to restore the default value.

distance *distance*

no distance

Parameter Description

Parameter	Description
distance	Sets the RIPng administrative distance. The range is from 1 to 254.

Defaults

The default distance is 120

Command mode

Routing process configuration mode.

Usage Guide

N/A

Configuration Examples

The following example shows how to set the RIPng administrative distance as 160:

```
FS(config)# ipv6 router rip
FS(config-router)# distance 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.4 distribute-list

Use this command to filter the in/out route in the prefix list. Use the **no** form of this command to remove route filtering.

distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

no distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

Parameter Description

Parameter	Description
prefix-list *prefix-list-name*	Name of the prefix list which is used to filter the route.
in | **out**	Filters the in or out route in the distribute list.
interface-type interface-name	(Optional) Applies the distribute list to the specified interface.

Defaults

By default, no distribute list is defined.

Command mode

Routing process configuration mode.

Usage Guide

This command is used to configure the route distribution control list to filter all update routes for the purpose of refusing to receive or send the specified routes. If the interface is not specified, the update routes on all interfaces are filtered.

Configuration Examples

The following example shows how to filter the received update route on the interface eth0 (only those update routes within the **prefix-list** *allowpre* prefix list range can be received)

```
FS(config)# ipv6 router rip
FS(config-router)# distribute-list prefix-list allowpre in eth0
```

Related Commands

Command	Description
redistribute	Sets route redistribution.

Platform Description

N/A

4.5 graceful-restart

Use this command to configure the graceful restart (GR) function for the RIPng process.

graceful-restart [**grace-period** *grace-period*]

Use the **no** form of this command restore the default configurations.

no graceful-restart [**grace-period**]

Parameter Description

Parameter	Description
graceful-restart	Enables the GR function.
grace-period	Displays the configured grace period.
grace-period	Indicates the configured GR period, ranging from 1 to 1800 seconds. The default value is the smaller between twice of the update time and 60s.

Defaults

The GR function is enabled by default.

Command Mode

Routing process configuration mode

Default Level

14

Usage Guide

The GR function is configured based on RIPng instances. Different parameters can be configured for different RIPng instances as required.

The GR period indicates the maximum duration from RIPng restart to RIPng GR completion. In this time period, the forwarding table before restart is used and the RIPng route is restored to the status before restart. After the GR period expires, the RIPng process exits the GR status and the common RIPng operation is performed.

The **graceful-restart grace-period** command allows a user to modify the GR period in explicit mode. Note that GR is completed and the RIPng route is updated once before the RIPng route becomes invalid. If the GR period is improperly set, continuous data forwarding in the GR process cannot be ensured. A typical case is as follows:

If the GR period is greater than the invalid time of the neighbor route, GR is not completed before the route becomes invalid and the route is not advertised to the neighbor again. The neighbor route stops forwarding data after the route becomes invalid, resulting in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the GR period needs to be configured, check configuration of the **timers** command to ensure that the GR period value is greater than the route update time and smaller than the route invalid time.

When GR is performed for the RIPng process, ensure that the network environment is stable.

Configuration Examples

The following example enables the GR function for the RIPng process and configures the GR period.

```
FS(config)# ipv6 router rip
FS(config-router)# graceful-restart grace-period 90
```

Verification

Run the **show ipv6 rip** command to check whether the GR function is configured and query the configured grace period.

Prompts

N/A

Common Errors N/A

Platform Description N/A

4.6 ipv6 rip default-information

Use this command to generate a default IPv6 route to the RIPng. Use the **no** form of this command to remove the default route.

ipv6 rip default-information { **only** | **originate**} [**metric** *metric-value*]

no ipv6 rip default-information

Parameter Description

Parameter	Description
only	Advertises the IPv6 default route only.
originate	Advertises both of the IPv6 default route and other routes.
metric *metric-value*	Sets the metric value for the default route. The valid range is from 1 to 15. The default metric is 1.

Defaults By default, no default route is configured.

Command mode Interface configuration mode

Usage Guide With this command configured on an interface, the interface advertises an IPv6 default route and the route itself is not to join the device route forwarding table and the RIPng route database.

To avoid the route loop, once this command has been configured on the interface, RIPng refuses to receive the default route update message advertised from the neighbor.

Configuration Examples The following example shows how to create a default route to the RIPng routing process on the interface ethernet0/0 and enable this interface to advertise the default route only:

```
FS(config)# interface ethernet 0/0
FS(config-if)# ipv6 rip default-information only
```

Related Commands

Command	Description
show ipv6 rip	Displays the RIPng process and statistics.
show ipv6 rip database	Displays the RIPng route.

Platform Description N/A

4.7 ipv6 rip enable

Use this command to enable the RIPng on the interface. Use the **no** form of this command to disable RIPng on the interface.

ipv6 rip enable

no ipv6 rip enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults It is disabled by default.

Command mode Interface configuration mode.

Usage Guide This command is used to add the RIPng interface. Before this command is configured, if the RIPng is not enabled, use this command to enable the RIPng automatically.

Configuration Examples The following example shows how to enable the RIPng on the interface 0/0:

```
FS(config)# interface ethernet 0/0
FS(config-if)# ipv6 rip enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.8 ipv6 rip metric-offset

Use this command to set the interface metric value. Use the **no** form of this command to remove the metric configurations.

ipv6 rip metric-offset *value*

no ipv6 rip metric-offset

Parameter Description

Parameter	Description
value	Sets the interface metric value on the interface. The valid range is from 1 to 16.

Defaults The default value is 1.

Command mode

Interface configuration mode.

Usage Guide

Before the route is added to the routing list, the interface metric value shall be upon the route metric. To this end, the interface metric value influences the route usage.

Configuration Examples

The following example shows how to set the metric value of the interface Ethernet 0/1 as 5:

```
FS(config)# interface ethernet 0/1
FS(config-if)# ipv6 rip metric-offset 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.9 ipv6 router rip

Use this command to create the RIPng process and enter routing process configuration mode. Use the **no** form of this command to remove the RIPng process.

ipv6 router rip

no ipv6 router rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No RIPng process is configured by default.

Command mode

Global configuration mode.

Usage Guide

N/A.

Configuration Examples

The following example shows how to create the RIPng process and enter routing process configuration mode:

```
FS(config)# ipv6 router rip
```

Related Commands

Command	Description
ipv6 rip enable	Enables the RIPng on the specified interface.

Platform

N/A

Description

4.10 passive-interface

Use this command to disable the interface to send update packets. Use the **no** form of this command to enable the interface to send update packets.

passive-interface { **default** | *interface-type interface-num* }

no passive-interface { **default** | *interface-type interface-num* }

Parameter Description

Parameter	Description
default	Enables the passive mode on all interfaces.
interface-type interface-num	Interface type and interface number.

Defaults

No passive interface is configured by default.

Command mode

Routing process configuration mode.

Usage Guide

You can use the **passive-interface default** command to enable the passive mode on all interfaces. Then use the **no passive-interface** *interface-type interface-num* command to remove the specified interface from the passive mode.

Configuration Examples

The following example shows how to enable the passive mode on all interfaces and remove interface ethernet 0/0 from the passive mode:

```
FS(config-router)# passive-interface default
FS(config-router)# no passive-interface ethernet 0/0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.11 redistribute

Use this command to redistribute the route of other routing protocols to RIPng. Use the **no** form of this command to remove the redistribution configuration.

redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static**} [**metric** *metric-value* | **route-map** *route-map-name*]

no redistribute { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static**} [**metric** *metric-value* | **route-map** *route-map-name*]

Parameter Description

Parameter	Description
bgp	Redistributes the BGP routes to RIPng.
connected	Redistributes the connected routes to RIPng.
isis [*area-tag*]	Redistributes the ISIS routes to RIPng. *area-tag* indicates the ISIS process number.
ospf *process-id*	Redistributes the OSPF routes to RIPng. *process-id* indicates the OSPF process number, and the range is from 1 to 65,535.
static	Redistributes the static routes to RIPng.
metric *metric-value*	(Optional) Sets the metric value for the route redistributed to RIPng.
route-map *route-map-name*	(Optional) Sets the redistribution route filtering.

Defaults

By default, the routes of other routing protocols are not redistributed.

If the **default-metric** command is not configured, the default metric value is 1;

By default, the **route-map** is not configured;

By default, all sub-type routes in the specified routing process are redistributed.

Command mode

Routing process configuration mode.

Usage Guide

This command is used to redistribute the external routes to RIPng.

It is unnecessary to transform the metric of one routing protocol into another routing protocol in the process of the route redistribution, for the metric calculation methods of the different routing protocols are different. The RIP and OSPF metric calculations are incomparable for the reason that the RIP metric calculation is hop-based while the OSPF one is bandwidth-based.

The instance, from where the routing information is redistributed to the RIPng, must be specified in the process of configuring the multi-instance protocol redistribution.

Configuration Examples

The following example shows how to redistribute the static route, use the route map *mymap* to filter and set the metric value as 8:

```
FS(config)# ipv6 router rip
FS(config-router)# redistribute static route-map
mymap metric 8
```

Related Commands

Command	Description
default-metric	Defines the default RIPng metric value when redistributing other routing protocols.
distribute-list	Filters the RIPng routing update packets.

Platform

N/A

Description

4.12 show ipv6 rip

Use this command to show the parameters and each statistical information of the RIPng routing protocol process.

show ipv6 rip

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode or user mode.

Usage Guide

N/A

Configuration Examples

```
FS# show ipv6 rip
Routing Protocol is "RIPng"
Sending updates every 10 seconds with +/-50%, next due in 8 seconds
Timeout after 30 seconds, garbage collect after 60 seconds
Outgoing update filter list for all interface is:
distribute-list prefix aa out
Incoming update filter list for all interface is: not set
Default redistribution metric is 1
Default distance is 120
Redistribution:
Redistributing protocol connected route-map rm
Redistributing protocol static
Redistributing protocol ospf 1
Default version control:    send version 1, receive version 1
Interface                  Send      Recv
VLAN 1                    1          1
Loopback 1                1          1
Routing Information Sources:
None
```

Related Commands

Command	Description
show ipv6 rip	Displays the parameters and each statistical information of the RIPng process.

Platform Description

N/A

4.13 show ipv6 rip database

Use this command to display the RIPng route entries.

show ipv6 rip database

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode or user mode.

Usage Guide

N/A

Configuration Examples

```
FS# show ipv6 rip database
Codes: R - RIPng,C - Connected,S - Static,O - OSPF,B - BGP
sub-codes:n - normal,s - static,d - default,r - redistribute,
i - interface, a/s - aggregated/suppressed
S(r)    2001:db8:1::/64, metric 1, tag 0
Loopback 0/::
S(r)    2001:db8:2::/64, metric 1, tag 0
Loopback 0/::
C(r)    2001:db8:3::/64, metric 1, tag 0
VLAN 1/::
S(r)    2001:db8:4::/64, metric 1, tag 0
Null 0/::
C(i)    2001:db8:5::/64, metric 1, tag 0
Loopback 1/::
S(r)    2001:db8:6::/64, metric 1, tag 0
```

```
Null 0/::
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.14 split-horizon

Use the **split-horizon** command to enable the RIPng split-horizon function in routing process configuration mode. Use the **no** form of this command to disable this function. Use the **split-horizon poisoned-reverse** command to enable the RIPng poisoned reverse horizontal split function in routing process configuration mode. Use the no form of this command to disable this function.

split-horizon [**poisoned-reverse**]

no split-horizon [**poisoned-reverse**]

Parameter Description

Parameter	Description
poisoned-reverse	(Optional) Enables the poisoned-reverse horizontal split.

Defaults RIPng split horizon is enabled by default.

Command mode Routing process configuration mode.

Usage Guide In the process of packet updating, split-horizon function prevents some routing information from being advertised through the interface learning those routing information. The poisoned reverse horizontal split function advertises some routing information to the interface learning those routing information, and the metric value is set as 16. The RIPng routing protocol belongs to the distance vector routing protocol, so the horizontal split shall be noticed in the actual application. You can use the **show ipv6 rip** command to determine whether the RIPng split-horizon function is enabled or not.

Configuration Examples The following example shows how to disable the RIPng horizontal split:

```
FS(config)# ipv6 router rip
FS(config-router)# no split-horizon
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

4.15 timers

Use this command to adjust the RIPng timer. Use the **no** form of this command to restore the default settings.

timers *update invalid flush*

no timers

Parameter Description

Parameter	Description
update	Sets the routing update time, in seconds. The update parameter defines the period of sending the routing update packets by the device. The invalid and flush parameter reset once the update packets are received.
invalid	Sets the routing invalid time, in seconds, starting from receiving the last valid update packet. The invalid parameter defines the invalid time for the un-updated routing in the routing list. The routing invalid time shall be three times larger than the routing update time. The routing will be invalid if no update packets are received within the routing invalid time, and it will reset if the update packets are received within the invalid time.
flush	Sets the routing flush time, in seconds, starting from RIPng entering to invalid state. The invalid routing will be removed from the routing list if the flush time expires.

Defaults

The default update time is 30 seconds; the default invalid time is 180 seconds; and the default flush time is 120 seconds.

Command mode

Routing process configuration mode.

Usage Guide

Adjusting the above time may speed up the RIPng convergence time and the troubleshooting time. The RIPng time must be consistent for the devices connecting to the same network. You are not recommended to adjust the RIP time, except for the specific requirement.

Use the **show ipv6 rip** command to view the current RIPng time parameter setting.

In the low-speed link, with the short time configured, large amount of the update packets consumes a lot of bandwidth. Generally, the short time can be configured in the Ethernet or 2Mbps-higher line to shorten the convergence time of the network routing.

Configuration Examples

The following example shows how to send the RIP update packets every 10 seconds. The routing will be invalid if no update packets are received within 30 seconds, and the routing will be removed after being invalid for 90 seconds.

```
FS(config)# ipv6 router rip
FS(config-router)# timers 10 30 90
```

Related Commands

Command	Description
show ipv6 rip	Displays the parameters and the statistical information of the RIPng process.
show ipv6 rip database	Displays the RIPng routes.

Platform Description N/A

5 OSPFv2 Commands

5.1 area

Use this command to configure the specified OSPF area. Use the **no** form of this command to restore the default setting.

area *area-id*

no area *area-id*

Parameter Description

Parameter	Description
area-id	ID of the OSPF area. The value can be a decimal integer or an IP address.

Defaults No OSPF area is configured by default.

Command Mode Routing process configuration mode

Usage Guide Use the no form of this command to remove the specified OSPF area and its configuration, including the area-based **area authentication, area default-cost, area filter-list, and area nssa** commands.

- Do not remove the OSPF area configuration under the following conditions:
- Virtual links exist in the backbone area. The virtual links must be removed at first.
- The corresponding network area command exists in any area. All network segment commands added to an area must be removed at first.

Configuration Examples The following example removes the configuration of OSPF area 2.

```
FS(config)# router ospf 2
FS(config-router)# no area 2
```

Related Commands

Command	Description
network area	Defines the interface where OSPF runs and the belonging area of the interface.

Platform Description N/A

5.2 area authentication

Use this command to enable OSPF area authentication. Use the **no** form of this command to restore the default setting.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication**

Parameter Description

Parameter	Description
area-id	Specifies ID of the area enabled with OSPF. The value can be a decimal integer or an IP address.
message-digest	(Optional) Enables MD5 (message digest 5) authentication mode.

Defaults No authentication is enabled by default.

Command Mode Routing process configuration mode

Usage Guide The FSOS software supports three authentication types:

1) 0, no authentication. The authentication type in the OSPF packet is 0when this command is not executed to enable OSPF authentication. 2) 1, plain text authentication mode. When this command is configured, the message-digest option is not used.3) 2, MD5 authentication mode. When this command is configured, the message-digest option is used.

All devices in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication password must be configured on an interface connecting neighbors. You can use the **ip ospf authentication-key** command to configure the plain text authentication password, and the **ip ospf message-digest-key** command to configure the MD5 authentication password in interface configuration mode.

Configuration Examples The following example uses MD5 authentication and the authentication password backbone in area 0 (backbone area) of the OSPF routing process.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip address 192.168.12.1 255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf message-digest-key 1 md5 backbone
FS(config)# router ospf 1
FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
FS(config-router)# area 0 authentication message-digest
```

Related Commands

Command	Description
ip ospf authentication-key	Defines the OSPF plain text authentication password.
ip ospf message-digest-key	Defines the OSPF MD5 authentication password.
area virtual-link	Defines a virtual link.

Platform Description N/A

5.3 area default-cost

Use this command to define the cost (OSPF metric) of the default aggregate route advertised to the stub area or not-so-stubby area (NSSA) in routing process configuration mode. Use the **no** form of this command to restore the default setting.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter Description

Parameter	Description
area-id	ID of the stub area or NSSA
cost	Cost of the default aggregate route advertised to the stub area or NSSA. The range is from 0 to 16777215.

Defaults

The default is 1.

Command Mode

Routing process configuration mode

Usage Guide

This command takes effect only on the Area Border Router (ABR) of the stub area or the ABR/Autonomous System Border Router (ASBR) of the NSSA.

The ABR can advertise a Link State Advertisement (LSA) indicating the default route in the stub area. The ABR/ASBR can advertise an LSA indicating the default route in the NSSA. You can use the **area default-cost** command to modify the LSA cost.

Configuration Examples

The following example sets the cost of the default aggregate route to 50.

```
FS(config)# router ospf 1
FS(config-router)# network 172.16.0.0 0.0.255.255 area 0
FS(config-router)#network 192.168.12.0 0.0.0.255 area 1
FS(config-router)# area 1 stub
FS(config-router)# area 1 default-cost 50
```

Related Commands

Command	Description
area stub	Sets an OSPF area as a stub area.
area nssa	Sets an OSPF area as an NSSA.

Platform Description

N/A

5.4 area filter-list

Use this command to filter the inter-area routes on the ABR. Use the **no** form of this command to restore the default setting.

area *area-id* **filter-list** { **access** *acl-name*| **prefix** *prefix-name* } { **in** | **out** }

no area *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name* } { **in** | **out** }

Parameter

Parameter	Description

Description

area-id	Area ID
acl-name	Name of an Access Control List (ACL)
prefix-name	Prefix-list name
in | **out**	Applies the ACL rule to the routes incoming/outgoing the area.

Defaults

No filtering is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

This command can be configured only on an ABR.

You can use this command when it is required to filter the inter-area routes on the ABR.

Configuration Examples

The following example sets area 1 to learn only the inter-area routes of 172.22.0.0/8.

```
FS# configure terminal
FS(config)# access-list 1 permit 172.22.0.0 0.255.255.255
FS(config)# router ospf 100
FS(config-router)# area 1 filter-list access 1 in
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.5 area nssa

Use this command to set an OSPF area as an NSSA in routing process configuration mode. Use the **no** form of this command to delete the NSSA or the NSSA configuration.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]

no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** | **always**]]

Parameter Description

Parameter	Description
area-id	NSSAID
no-redistribution	Imports the routing information to a common area other than the NSSA for the NSSA ABR.
default-information originate	Generates and imports the default Type 7 LSA to the NSSA. This option takes effect only on the NSSA ABR or ASBR.
metric *value*	Sets the metric of the generated default LSA. The range is from 0 to 16777214.

	The default value is 1.
metric-type *type*	Sets the type of the generated LSA to N-1 or N-2. The default value is N-2.
no-summary	Prevents the NSSA ABR from sending summary LSAs (Type-3 LSA).
translator	Configures the translator for the NSSA ABR.
stability-interval *seconds*	Configures the stability interval in seconds for the NSSA ABR that functions as a translator to change to a non-translator. The range is from 0 to 2147483647. The default value is 40.
always	Configures that an NSSA ABR always functions as a translator. The NSSA ABR is the backup translator by default.

Defaults

No NSSA is defined by default.

Command Mode

Routing process configuration mode

Usage Guide

The default-information-originate parameter is used to generate the default Type-7 LSA. However, on the NSSA ABR, the default Type-7 LSA will always be generated; On the ASBR (which is not an ABR at the same time), the default Type-7 LSA is generated only when the default route exists in the routing table.

The no-redistribution parameter prevents the OSPF from advertising the external routes imported with the redistribute command to the NSSA on the ASBR. This option is generally used when the NSSA device is both an ASBR and an ABR.

To reduce the number of LSAs sent to the NSSA, you can configure the no-summary parameter on the ABR to prevent it from advertising summary LSAs (Type-3 LSAs) to the NSSA. In addition, you can use the area default-cost command on the NSSA ABR to configure the cost of the default route advertised to the NSSA. By default, this cost is 1.

If an NSSA has multiple ABRs, the ABR with the greatest ID is selected as the Type-7 or Type-5 translator. To configure that an NSSA ABR always functions as a translator, you can use the translator always parameter. If the translator role of an ABR is taken away by another ABR, the ABR still possesses the conversion capability within stability-interval. If the ABR fails to take back its translator role when stability-interval expires, the LSA that changes from Type-7 to Type-5 will be removed from the autonomous domain.

To avoid route loops, Type-5 LSAs generated from Type-7 convergence will be eliminated immediately after the current device stopped serving as a translator, with no need to wait until the stability-interval expires.

In a same NSSA, you are recommended to configure the **translator always** parameter on only one ABR.

When the Type-7 LSAs are translated to Type-5, forwarding addresses (FA) of Type-7 LSAs are included in the translated Type-5 LSAs.

Configuration Examples

The following example sets area 1 as an NSSA on all routers of the area.

```
FS(config)#router ospf1
FS(config-router)#network 172.16.0.0 0.0.255.255 area0
FS (config-router)#network 192.168.12.0 0.0.0.255 area 1
FS(config-router)# area1nssa
```

Related Commands

Command	**Description**

area default-cost	Defines the cost (OSPF metric) of the default aggregate route advertised to the NSSA.

Platform Description

N/A

5.6 area range

Use this command to configure inter-area route aggregation for OSPF. Use the **no** form of this command to delete route aggregation. Use the **no** form with the cost parameter to restore the default metric of the aggregate route, but not delete route aggregation.

area *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [c**ost** *cost*]

no area *area-id* **range** *ip-address net-mask* [cost]

Parameter Description

Parameter	Description
area-id	ID of the area where the aggregate route is injected into. The value can be a decimal integer or an IP address.
ip address net-mask	Network segment whose routes are to be aggregated
advertise | not-advertise	Whether to advertise the aggregate route
cost *cost*	Sets the priority of the interface. The range is from 0 to 16777215.

Defaults

No inter-area route aggregation is configured by default.

The configured aggregation range is advertised by default.

The default metric of the aggregate route depends on whether the device is compatible with RFC1583. If yes, the default metric is the smallest cost of the aggregate route. If no, the default metric is the largest cost of the aggregate route.

Command Mode

Routing process configuration mode

Usage Guide

This command takes effect only on the ABR to aggregate multiple routes of an area into a route and advertise it to other areas. Route combination occurs only on the border of an area. The devices inside an area see the specific routing information, but the devices outside the area see only one aggregate route. The advertise and not-advertise options can set whether to advertise the aggregate route for filtering and masking. The aggregate route is advertised by default.

You can use the cost option to set the metric of the aggregate route.

You can define route aggregate in multiple areas to simplify the routes in the whole OSPF routing area. This improves the network forwarding performance, especially in large networks.

The area range of route aggregation is determined according to the longest match when multiple aggregate routes with direct inclusion relationships are configured.

Configuration Examples

The following example aggregate the routes of area 1 into a route 172.16.16.0/20.

```
FS(config)#router ospf 1
FS(config-router)#network 172.16.0.0 0.0.15.255area0
FS((config-router)#network 172.16.17.0 0.0.15.255area1
FS(config-router)#area1range 172.16.16.0 255.255.240.0
```

Related Commands

Command	Description
discard-route	Enables a discarded route to be added to a routing table.
summary-address	Configures the OSPF external route aggregation.

Platform Description N/A

5.7 area stub

Use this command to set an OSPF area as a stub area or full stub area. Use the **no** form of this command to restore the default setting.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter Description

Parameter	Description
area-id	Stub area ID
no-summary	(Optional) Prevents the ABR from advertising the network summary link to the stub area. Here the stub area is called the full stub area. Only the ABR needs this parameter.

Defaults No stub area is defined by default.

Command Mode Routing process configuration mode

Usage Guide All devices in the OSPF stub area must be configured with the area stub command. The ABR only sends three types of link state advertisement (LSA) to the stub area: 1) type 1, device LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. For the routing table, the devices in the stub area can learn only the routes inside the OSPF routing domain, including the internal default routes generated by the ABR.

To configure a full stub area, use the area stub command with the no-summary keyword on the ABR. The devices in the full stub area can learn only the routes in the local area and the internal default routes generated by the ABR.

Two commands can configure an OSPF area as a stub area: the area stub and area default-cost commands. All devices connected to the stub area must be configured with the area stub command, but the area default-cost command can be executed only on the ABR. The area default-cost command defines the initial cost (metric) of the internal default route.

Configuration Examples

The following example sets area 1 as the stub area on all devices in area 1.

```
FS(config)# router ospf1
FS(config-router)# network172.16.0.0 0.0.255.255 area 0
FS (config-router)# network 192.168.12.0     0.0.0.255 area 1
FS(config-router)# area 1 stub
```

Related Commands

Command	Description
area default-cost	Defines the cost (OSPF metric value) of the default aggregate route advertised to the stub area.

Platform Description

N/A

5.8 area virtual-link

Use this command to define the OSPF virtual link in routing process configuration mode. Use the **no** form of this command to restore the default setting.

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*]]

no area *area-id* **virtual-link** *router-id* [**authentication**] [**dead-interval**] [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [[**authentication-key**] | [**message-digest-key** *key-id]]*

Parameter Description

Parameter	Description
area-id	ID of the OSPF transition area. The value can be a decimal integer or an IP address.
router-id	ID of the router neighboring to the virtual link. It can be viewed with the show ip ospf command.
dead-interval *seconds*	(Optional) Defines the time to declare neighbor loss in seconds. The range is 0 to 2147483647.This value must be consistent with that of the neighbor.
minimal	Enables the Fast Hello function and sets the death clock to 1 second.
hello-multiplier	Multiplies dead-interval with hello-interval in the Fast-Hello function.
multiplier	Specifies the number of Hello packets that are sent every second in the Fast Hello function. The range is from 3 to 20.
hello-interval *seconds*	(Optional)Defines the interval at which the HELLO packet is sent by the OSPF to the virtual link in seconds. The range is from1 to 65535.This value must be consistent with that of the neighbor.
retransmit-interval *seconds*	(Optional) OSPF LSA retransmission interval in seconds. The range is from 0 to 65535. The parameter setting must consider the round-trip time of packets on the link.
transmit-delay *seconds*	(Optional) OSPF LSA transmission delay in seconds. The range is from 0 to 65535. This value adds the LSA keep alive period. When the LSA keep alive

	period reaches a threshold, the LSA will be refreshed.
authentication-key [0|7]*key*	(Optional) Defines the OSPF plain text authentication key. The plain text authentication key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
message-digest-key *key-id***md5 [0|7**]*key*	(Optional) Defines the OSPF MD5 authentication key and key ID. The MD5 authentication key ID and key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
authentication	Sets the authentication type to plain text.
message-digest	Sets the authentication type to MD5.
null	Sets the authentication type to no authentication.

Defaults

The following are the default values:
dead-interval: 40seconds
hello-interval: 10seconds
retransmit-interval: 5seconds
transmit-delay: 1second
authentication: null
The Fast Hello function is disabled by default.
The other parameters do not have default values.

Command Mode

Routing process configuration mode

Usage Guide

A virtual link can connect an area to the backbone area, or another non-backbone area. In the OSPF routing domain, all areas must connect to the backbone area. If an area disconnects from the backbone area, a virtual link to the backbone area is required. Otherwise, the network communication will become abnormal. The virtual link is created between two ABRs. The area that belongs to both ABRs is called the transition area, which can never be a stub area or NSSA.

The router-id parameter indicates the ID of OSPF neighbor router and can be displayed with the show ip ospf neighbor command. You can configure the loopback address as the router ID.

The area virtual-link command defines only the authentication key for a virtual link. You can use the area authentication command to enable the OSPF packet authentication in areas connected over the virtual link in routing process configuration mode.

OSPF supports the Fast Hello function.

If the Fast Hello function is enabled, the OSPF can discover neighbors and detects invalid neighbors quickly. You can enable the OSPF Fast Hello function by specifying the keywords minimal and hello-multiplier, and the multiplier parameter. You can set the death clock to 1 second in minimal and hello-multiplier to a value equal to or greater than 2. In this case, the Hello packet sending interval is less than 1 second.

The hello-interval field of a Hello packet received by a virtual link is omitted if the Fast Hello function is enabled on the virtual link and the hello-interval field is set to 0 for Hello packets advertised from the virtual link.

No matter the Fast Hello function is enabled or not, the values of dead-interval must be consistent on both ends of a virtual link. The values of hello-multiplier on both ends can be different if at least one Hello packet can be received within dead-interval. You can use the show ip ospf virtual-links command to monitor dead-interval and hello-interval configured for a virtual link.

For the Fast Hello function, you can only configure either the **dead-interval minimal hello-multiplier** parameter or the **hello-interval** parameter.

Configuration Examples

The following example sets area 1 as the transition area to establish virtual link with neighbor *2.2.2.2*.

```
FS(config)# router ospf 1
FS(config-router)# network 172.16.0.0 0.0.15.255 area0
FS(config-router)# network 172.16.17.0 0.0.15.255 area1
FS(config-router)#area1 virtual-link2.2.2.2
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor *1.1.1.1*. This virtual link connects area 10 and the backbone area, and works with the OSPF packet authentication inMD5 mode.

```
FS(config)# routerospf1
FS(config-router)# network172.16.17.0 0.0.15.255area1
FS(config-router)# network172.16.252.0 0.0.0.255 area10
FS(config-router)# area 0 authentication message-digest
FS(config-router)# area1virtual-link 1.1.1.1message-digest-key1md5hello
```

The following example sets area 1 as the transition area to establish a virtual link with neighbor 1.1.1.1, enables the Fast Hello function on this virtual link, and sets the multiplier to 3.

```
FS(config)# routerospf1
FS(config-router)# network172.16.17.0 0.0.15.255 area1
FS(config-router)# network 172.16.252.0 0.0.0.255 area10
FS(config-router)# area1 virtual-link1.1.1.1dead-interval minimal hello-multiplier 3
```

Related Commands

Command	**Description**
area authentication	Enables the OSPF area packet authentication and define the authentication mode.
show ip ospf	Displays the OSPF process information, including the router ID.
show ip ospf virtual-links	Monitors information about a virtual link.

Platform Description

N/A

5.9 auto-cost

Use this command to enable the auto-cost function and set the reference bandwidth according to the reference bandwidth. Use the **no** form of this command to restore the default setting.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter Description

Parameter	Description
ref-bw	Reference bandwidth, in the range from1 to 4294967 Mbps.

Defaults

The default is 100Mbps.

Command Mode

Routing process 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.

Configuration Examples

The following example configures the reference bandwidth as 10 Mbps.

```
FS(config)# routerospf1
FS(config-router)# network172.16.10.0 0.0.0.255 area0
FS(config-router)# auto-costreference-bandwidth10
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information
ip ospf cost	Sets the cost value of the OSPF interface.
bandwidth	Sets the interface bandwidth. This setting does not affect data transmission rate.

Platform Description

N/A

5.10 capability opaque

Use this command to enable Opaque LSA. Use the **no** form of this command to disable this function.

capability opaque

no capability opaque

Parameter Description

Parameter	Description
N/A	N/A

Defaults Opaque LSA is enabled by default.

Command Mode Routing process configuration mode.

Usage Guide N/A

Configuration Examples The following example disables Opaque LSA capability.

```
FS(config)# router ospf 1
FS(config-router)# no capability opaque
```

Related Commands

Command	Description
show ip ospf	Displays the global configuration of OSPF.

Platform Description N/A

5.11 clear ip ospf process

Use this command to clear and restart the OSPF instance.

clear ip ospf *(process-id)* **process**

Parameter Description

Parameter	Description
process-id	OSPF instance ID. When the ID is specified, the command clears data related to the specified instance and restarts the OSPF instance. When no ID is specified, the command clears data related to all running OSPF instances and restarts all the running OSPF instances.

Defaults The rule recommended in the RFC 1583 is used by default.

Command Mode Privileged EXEC mode

Usage Guide Resetting the entire OSPF process causes that all neighbors are re-established and OSPF is greatly affected. Therefore, you are prompted to confirm the execution for deliberation.

Configuration Examples

The following example clears data of OSPF instance 1 and restarts OSPF instance 1.

```
FS#clearipospf1process
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.12 compatible rfc1583

Use this command to determine the RFC 1583 or RFC 2328 rule for selecting the optimal route among route table several routes to the same destination out of the Autonomous System (AS).

compatible rfc1583

no compatible rfc1583

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The RFC 1583 rule is used by default.

Command Mode

Routing process configuration mode

Usage Guide

N/A

Configuration Examples

The following example determines the best route with the RFC 2328 rule.

```
FS(config)# routerospf1
FS(config-router)# nocommpatiblerfc1583
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information

Platform Description

N/A

5.13 default-information originate

Use this command to generate a default route to be injected into the OSPF routing domain in routing process configuration mode. Use the **no** form of this command to restore the default setting.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map-name*]

Parameter Description

Parameter	**Description**
always	(Optional) Generates the default route unconditionally, no matter whether the default route exists locally or not.
metric *metric*	(Optional) Initial metric of the default route in the range from0 to 16777214
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics on different devices; type 2, same metric on different devices. An external route of type 1 is more trustworthy than that of type 2.
route-map *map-name*	Associated route map name. No route map is associated by default.

Defaults

No default route is generated by default.

The default value of metric is 1.

The default value of metric-type is 2.

Command Mode

Routing process configuration mode

Usage Guide

When the **redistribute** or **default-information** command is executed, the OSPF-enabled device automatically turns into the ASBR. The ASBR cannot generate the default route automatically or advertise it to all the devices in the OSPF routing domain. The ASBR can generate the default route with the **default-information originate** command in routing process configuration mode.

If the always parameter is used, the OSPF routing process advertises an external default route to neighbors, no matter the default route exists or not. However, the local device does not display the default route. To make sure whether the default route is generated, use the **show ip ospf database** command to display the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. You can use the show ip route command on the OSPF neighbor to display the default route.

The metric of the external default route can be defined only with the **default-information originate** command.

There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, the type 1 route takes precedence over the type 2 route. As a result, the **show ip route** command displays only the type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area.

To generate a default route in the NSSA area, use the **area nssa default-information-originate** command.

The routers in the stub area cannot generate external default routes.

⚠ The range of set metric is 0 to 16777214 for the associated route map. If the value exceeds the range, introducing a route fails.

Configuration Examples

The following example configures that OSPF generates an external default route and injects it to the OSPF routing domain. The default route is of type 1 and the metric 50.

```
FS(config)#routerospf 1
FS(config-router)#network172.16.24.0 0.0.0.255 area 0
FS(config-router)#default-information originate
alwaysmetric50metric-type1
```

Related Commands

Command	Description
show ip ospf database	Displays OSPF link state database.
show ip route	Displays the IP route table.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

5.14 default-metric

Use this command to set the **default metric** of OSPF redistribution route. Use the **no** form of this command to restore the default setting.

default-metric *metric*

no default-metric

Parameter Description

Parameter	Description
metric	Default metric of the OSPF redistribution route in the range from1 to 16777214

Defaults The default metric is not configured by default.

Command Mode Routing process configuration mode

Usage Guide The **default-metric** command must work with the **redistribute** command in routing process configuration mode to modify the initial metric of all redistributed routes.

The configuration result of the **default-metric** command does not take effect for the external routes injected into the OSPF routing domain with the **default-information originate** command.

Configuration Examples The following example configures the default metric of the OSPF redistribution route as 50.

```
Switch(config)# router rip
FS(config-router)# network192.168.12.0
Switch(config-router)# version 2
FS(config-router)# exit
FS(config)# routerospf1
FS(config-router)# network172.16.10.0 0.0.0.255area0
Switch(config-router)# default-metric 50
FS(config-router)# redistribute rip subnets
```

Related Commands

Command	Description
redistribute	Redistributes the routes of other routing processes.
show ip ospf	Displays the OSPF global configuration information.

Platform Description

N/A

5.15 discard-route

Use this command to enable adding the discard-route into the core route table. Use the **no** form of this command to disable this function.

discard-route { **internal | external** }

no discard-route { **internal** | **external** }

Parameter Description

Parameter	Description
internal	Enables adding the discard-route generated with the area range command
external	Enables adding the discard-route generated with the summary-address command.

Defaults

Adding the discard-route is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

After route aggregation, the range may exceed the actual network range of the route table, and sending the data to the nonexistent network may cause loops or increase router loads. To prevent this situation, the discard-route is added to the route table on the ABR or the ASBR. The discard-route is generated automatically and will not be transmitted.

Configuration Examples

The following example disables adding the discard routes generated with the area range command.

```
FS(config)# router ospf 1
FS(config-router)# no discard-route internal
```

Related Commands

Command	Description
area range	Configures the route aggregation between OSPF areas.
summary-address	Configures the route aggregation out of the OSPF routing domain.

Platform

N/A

Description

5.16 distance ospf

Use this command to set the Administration Distance (AD) of different types of OSPF routes. Use the **no** form of this command to restore the default setting.

distance { *distance* | **ospf** { [**intra-area** *distance*] [**inter-area** *distance*] [**external** *distance*] } }

no distance [**ospf**]

Parameter Description

Parameter	Description
distance	Sets the route AD in the range from1 to 255.
intra-area *distance*	Sets the AD of the intra-area route in the range from1 to 255.
inter-area *distance*	Sets the AD of the inter-area route in the range from1 to 255.
External *distance*	Sets the AD of the external route in the range from1 to 255.

Defaults

The default value is 110.

The default intra-area distance is 110.

The default inter-area distance is 110.

The default external distance is 110.

Command Mode

OSPF Routing process configuration mode

Usage Guide

This command is used to specify different ADs for different types of OSPF routes.

Configuration Examples

The following example sets the OSPF external route AD to 160.

```
FS(config)# routerospf1
FS(config-router)# distance ospf external 160
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.17 distribute-list in

Use this command to configure LSA filtering. Use the **no** form of this command to restore the default setting.

distribute-list *{ [access-list-number | name] | prefix prefix-list-name [* **gateway** *prefix-list-name] |* **route-map** *route-map-name } in [interface-type interface-number]*

no distribute-list *{ [access-list-number | name] | prefix prefix-list-name [* **gateway** *prefix-list-name] |* route-map *route-map-name } in [interface-type interface-number]*

Parameter Description

Parameter	Description
access-list-number | **name**	Uses the ACL filtering rule.
gateway *prefix-list-name*	Uses the gateway filtering rule.
Prefix *prefix-list-name*	Uses the prefix-list filtering rule.
route-map *route-map-name*	Uses the route-map filtering rule.
interface-type interface-number	Configures the LSA route filtering on the interface.

Defaults

No filtering is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the Shortest Path First (SPF) calculation to generate the corresponding routes. It does not affect the link status database or the route table of the neighbors. It only affects the routing entries calculated by local OSPF. This function is used to control routes that enter the ABR or ASBR.

The following route-map rules will be supported if the route-map parameter is configured:

match interface

match ip address

match ip address prefix-list

match ip next-hop

match ip next-hop prefix-list

match metric

match route-type

match tag

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 Examples

The following example configures LSA filtering.

```
FS(config)# access-list3permit172.16.0.00.0.127.255
FS(config)# router ospf 25
FS(config-router)# distribute-list 3 in ethernet 0/1
```

Related Commands

Command	Description
distribute-list out	Filters redistribution routes.

Platform Description

N/A

5.18 distribute-list out

Use this command to configure filtering redistribution routes. The function is similar to that of the **redistribute** command. Use the **no** form of this command to restore the default setting.

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-nam*e } **out** [**connected | ospf** *process-id* **| rip | static**]

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-nam*e } **out** [**connected** | **ospf** *process-id* | **rip | static**]

Parameter Description

Parameter	Description
access-list-number | name	Uses the ACL filtering rule.
prefix prefix-list-name	Uses the prefix-list filtering rule.
connected | ospf process-id | **rip | static**	Source of the routes to be filtered

Defaults

No filtering is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

Similar to the redistribute route-map command, the distribute-list out command filters the routes that other protocols redistribute to the OSPF. However, the distribute-list out command does not redistribute routes by itself. It works with the redistribute command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration, that is, the two rules cannot be configured at the same time for routes from the same source.

Configuration Examples

The following example filters the redistributed static routes.

```
FS(config)# routerospf1
FS(config)# redistribute static subnets
FS(config-router)# distribute-list 22 outstatic
FS(config-router)# distribute-list prefix jjj out static
% Access-list filter exists, please de-config first
```

Related Commands

Command	Description
distribute-list in	Configures LSA filtering.
redistribute	Redistributes routes of other routing processes.

Platform Description

N/A

5.19 enable mib-binding

Use this command to bind the Management Information Base (MIB) with the specified OSPFv2 process. Use the **no** form of this command to restore the default setting.

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults The MIB is bound with the OSPFv2 process with the smallest ID by default.

Command Mode Routing process configuration mode

Usage Guide OSPFv2 MIB has no OSPFv2 process information, so the user operates a sole OSPFv2 process by SNMP. By default, OSPFv2 MIB is bound with the OSPFv2 process with the smallest ID. User operations take effect for this process. To operate the specified OSPF process over Simple Network Management Protocol(SNMP), use this command to bind the MIB to SNMP.

Configuration Examples The following example operates OSPFv2 process 100 over SNMP:

```
FS(config)# routerospf100
FS(config-router)# enable mib-binding
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.
enable traps	Configures the OSPF TRAP function.

Platform Description N/A

5.20 enable traps

The OSPFv2 process supports 16 kinds of TRAP packets, which are classified into four categories. Use this command to enable sending the specified TRAP messages. Use the **no** form of this command to restore the default setting.

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**]]

no 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

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><b>error</b></td><td>Configures all traps switches related to errors. Use this parameter to set the following specified error traps switches.
<table>
<tr><td><b>Ifauthfailure</b></td><td>Interface authentication error</td></tr>
<tr><td><b>Ifconfigerror</b></td><td>Interface parameter configuration error</td></tr>
<tr><td><b>Ifrxbadpacket</b></td><td>Error packets received on the interface</td></tr>
<tr><td><b>Virtifauthfailure</b></td><td>Authentication error on the virtual interface</td></tr>
<tr><td><b>Virtifconfigerror</b></td><td>Parameter configuration error on the virtual interface</td></tr>
<tr><td><b>Virtifrxbadpacket</b></td><td>Error packets received on the virtual interface</td></tr>
</table></td></tr>
<tr><td><b>isa</b></td><td>Configures all traps switches related to the LSA. Use this parameter to set the following specified LSA traps switches.
<table>
<tr><td><b>Lsdbapproachoverflow</b></td><td>External LSA count has reached the 90% of the upper limit.</td></tr>
<tr><td><b>Lsdboverflow</b></td><td>External LSA count has reached the upper limit.</td></tr>
<tr><td><b>Maxagelsa</b></td><td>LSA reaching the aging time</td></tr>
<tr><td><b>Originatelsa</b></td><td>Generates new LSA</td></tr>
</table></td></tr>
<tr><td><b>retransmit</b></td><td>Configures all traps switches related to the retransmission. Use this parameter to set the following specified retransmit traps switches.
<table>
<tr><td><b>Iftxretransmit</b></td><td>Packet retransmission on the interface</td></tr>
<tr><td><b>Virtiftxretransmit</b></td><td>Packet retransmission on the virtual interface</td></tr>
</table></td></tr>
<tr><td><b>state-change</b></td><td>Configures all traps switches related to the state change. Use this parameter to set the following specified state-change switches.
<table>
<tr><td><b>Ifstatechange</b></td><td>Interface state change</td></tr>
<tr><td><b>NbrRestartHelper StatusChange</b></td><td>State change during the neighbor GR process</td></tr>
<tr><td><b>Nbrstatechange</b></td><td>Neighbor state change</td></tr>
<tr><td><b>NssaTranslatorStatusChange</b></td><td>State change of the NSSA translator</td></tr>
<tr><td><b>RestartStatusChange</b></td><td>State change of the GR Restarter on the device</td></tr>
<tr><td><b>Virtifstatechange</b></td><td>State change on the virtual interface</td></tr>
<tr><td><b>VirtNbrRestartHelper StatusChange</b></td><td>Status change of the virtual neighbor GR process</td></tr>
<tr><td><b>Virtnbrstatechange</b></td><td>State change on the virtual neighbor</td></tr>
</table></td></tr>
</table>

Defaults All TRAP switches are disabled by default.

Command Mode Routing process configuration mode

Usage Guide The **snmp-server enable traps ospf** command must be configured before you configure this command, for it is limited by the **snmp-server** command.

This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.

Configuration Examples The following example enables all TRAP switches of OSPFv2 process 100.

```
FS(config)# routerospf100
FS(config-router)# enable traps
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.
enable mib-binding	Binds the OSPFv2 process with MIB.
snmp-server enable traps ospf	Enables the OSPF TRAP notification function.

Platform Description N/A

5.21 graceful-restart

Use this command to enable the graceful restart (GR) of OSPF on the device. Use the **graceful-restart grace-period** command to configure the grace period parameter and enable the OSPF GR function. Use the **no** form of this command to disable this function.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [**graceful-period**]

Parameter Description

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.

Defaults This function is enabled by default.

Command Mode Routing process configuration mode

Usage Guide

GR is configured based on the OSPF instance. Different instances could be configured with different parameters according to the actual situation.

The graceful restart interval is the longest time between the OSPF restart and the graceful restart. In this period, you can perform link status reconstruction to restore the OSPF status to the original. With the interval times out, the OSPF will exit GR and perform common OSPF operations.

The GR interval is 120 seconds set with the graceful-restart command, and the graceful-restart grace-period command allows you to change the interval explicitly.

GR is unavailable when the Fast Hello function is enabled.

Configuration Examples

The following example enables GR for the OSPF instance 1 and sets the restart interval for GR.

```
FS(config)# router ospf 1
FS(config-router)# graceful-restart
FS(config-router)# graceful-restart grace-period 60
```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPF graceful-restart helper.

Platform Description

N/A

5.22 graceful-restart helper

Use this command to enable the graceful restart helper function. Use the **no** form of this command to restore the default setting.

graceful-restart helper disable

no graceful-restart helper disable

graceful-restart helper { **strict-lsa-checking** | **internal-lsa-checking**}

no graceful-restart helper {**strict-lsa-checking** | **internal-lsa-checking**}

Parameter Description

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.

Defaults

The GR helper is enabled by default.

The router enabled with the GR helper does not check the LSA change by default.

Command Mode

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 Examples

The following example disables the GF helper and modifies the policy of checking network changes.

```
FS(config)# router ospf1
FS(config-router)# graceful-restart helper disable
FS(config-router)# no graceful-restart helper disable
FS(config-router)# graceful-restart helper
strict-lsa-checking
```

Related Commands

Command	Description
graceful-restart	Enables GR on the device.

Platform Description

N/A

5.23 ip ospf authentication

Use this command to configure the authentication type. Use the **no** form of this command to restore the default setting.

ip ospf authentication [**message-digest** | **null**]

no ip ospf authentication

Parameter Description

Parameter	Description
message-digest	Enables MD5 authentication on the interface.
null	Enables no authentication.

Defaults

No authentication mode is configured and that of the local area is used on the interface by default.

Command Mode

Interface configuration mode

Usage Guide

Plaintext authentication is applicable when **no** option is used with the command. Note that the no form of this command restores the default value. Whether authentication is used actually depends on authentication mode configured for the local area of the interface. If authentication mode is configured as **null,** no authentication is enabled. When both the interface and its area are configured with authentication, the one for the interface takes precedence.

Configuration Examples

The following example configures MD5 authentication for OSPF on fastEthernet 0/1.

```
FS (config)#interface fastEthernet0/1
FS(config-if-FastEthernet 0/1)# ipaddress172.16.1.1
255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf authentication
message-digest
```

Related Commands

Command	Description
area authentication	Enables authentication and defines authentication mode in the OSPF area.
ip ospf authentication-key	Configures the plain text authentication key.
ip ospf message-digest-key	Configures the MD5 authentication key.

Platform Description

N/A

5.24 ip ospf authentication-key

Use this command to configure the OSPF plain text authentication key in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf authentication-key [**0 | 7**] *key*

no ip ospf authentication-key

Parameter Description

Parameter	Description
0	Displays the key in plain text.
7	Displays the key in cipher text.
key	Key containing at most eight characters.

Defaults

It is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

The **ip ospf authentication-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys may vary by interface, but the devices that are connected to the same physical network segment must use the same key.

To enable the OSPF area authentication, execute the area authentication command in routing process configuration mode.

The authentication can be enabled separately on an interface by executing the ip ospf authentication command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

Configuration Examples

The following example configures the OSPF authentication key ospfauth for fast Ethernet *0/1*.

```
FS (config)#interfacefastEthernet0/1
FS(config-if-FastEthernet 0/1)# ipaddress172.16.1.1
255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf authentication-key ospfauth
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode
ip ospf authentication	Enables authentication on the interface and defines authentication mode

Platform Description

N/A

5.25 ip ospf cost

Use this command to configure the cost (OSPF metric) of the OSPF interface for sending a packet in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf cost *cost*

no ip ospf cost

Parameter Description

Parameter	Description
cost	OSPF interface cost in the range from 0 to 65535

Defaults

The default interface cost is calculated as follows:

Reference bandwidth/Bandwidth

The reference bandwidth is *100* Mbps by default.

Command Mode

Interface configuration mode

Usage Guide

By default, the OSPF interface cost is 100Mbps/Bandwidth, where Bandwidth is the interface bandwidth configured with the bandwidth command in interface configuration mode.
The default costs of different types of lines are as follows:

- 64K serial line: 1562
- E1 line: 48
- 10M Ethernet: 10
- 100M Ethernet: 1

The OSPF cost configured with the **ip ospf cost** command will overwrite the default configuration.

Configuration Examples

The following example configures the OSPF cost of fastEthernet 0/1 to100.

```
FS(config)# interfacefastEthernet0/1
FS(config-if-FastEthernet 0/1)# ipospfcost100
```

Related Commands

Command	Description
bandwidth	Specifies the interface bandwidth. This setting does not affect the data transmission rate.
show ip ospf	Displays the OSPF global configuration information

Platform Description

N/A

5.26 ip ospf database-filter all out

Use this command to stop advertising LSAs of an interface, that is, the LSA update packets are not sent on the interface. Use the **no** form of the command to restore the default setting.
ip ospf database-filter all out
no ip ospf database-filter

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled and all LSA update packets can be sent on the interface by default.

Command Mode

Interface configuration mode

Usage Guide

To stop sending LSA update packets on the interface, enable this function on the interface.
Then, the device maintains the neighboring connections and accepts LSAs from neighbors, but stops sending LSAs to neighbors.

Configuration Examples

The following example stops sending LSA update packets of fastEthernet 0/1.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf database-filter all out
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.27 ip ospf dead-interval

Use this command to configure the interval for determining the death of an interface neighbor in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf dead-interval { *seconds* **| minimal hello-multiplier** *multiplier* }

no ip ospf dead-interval

Parameter Description

Parameter	Description
seconds	Defines the interval for determining the neighbor death in seconds. The range is from 0 to 2,147,483,647.
minimal	Indicates that the Fast Hello function is enabled to set the dead interval to 1s.
hello-multiplier *multiplier*	Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20.

Defaults

The value of dead-interval is 4 times the interval configured with the **ip ospf hello-interval** command by default.

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.

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 Examples

The following example configures the interval for determining the death of the OSPF neighbor on fastEthernet 0/1 to30seconds.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf dead-interval30
```

The following example configures the value of hello-multiplier to3.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf dead-interval minimal hello-multiplier 3
```

Related Commands

Command	Description
ip ospf hello-interval	Specifies the interval at which the OSPF sends Hello packets
show ip ospf interface	Displays OSPF interface information.

Platform Description

N/A

5.28 ip ospf disable all

Use this command to prevent the specified interface from generating OSPF packets. Use the **no** form of this command to restore the default setting.

ip ospf disable all

no ip ospf disable all

Parameter Description

Parameter	Description
N/A	N/A

Defaults

OSPF packets are generated on the specified interface by default.

Command Mode

Interface configuration mode

Usage Guide

The interface configured with this command will ignore whether the network areas are matched. After this command is configured, an interface will not generate OSPF packets even if the interface belongs to the network; therefore, the interface does not receive or send any OSPF packets or participate in OSPF calculation.

Configuration Examples

The following example prevents the specified interface from generating OSPF packets.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip address172.16.10.1 255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf disable all
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.29 ip ospf hello-interval

Use this command to set the interval for sending Hello packets in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameter Description

Parameter	Description
seconds	Interval for sending Hello packets in seconds. The range is from1 to 65535.

Defaults

The defaults are as follows:

10secons for Ethernet

10seconsfor PPP or HDLC encapsulated interfaces

10secons for frame relay PTP interfaces

30secons for non-frame relay PTP sub-interface and X.25 interfaces

Command Mode

Interface configuration mode

Usage Guide

The interval of sending the Hello packets is included in the Hello packet. A shorter interval means that OSPF detects the topological change faster, which will increase network traffic. The Hello packet sending intervals for all the devices in the same network segment must be the same. To manually modify the interval to determine neighbor death, ensure that the Hello packet sending interval cannot be greater than dead-interval of the neighbor.

Configuration Examples

The following example configures the interval of sending the Hello packets on fastEthernet 0/1 to15.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip address172.16.10.1 255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf hello-interval15
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the interval for determining the death of the OSPF neighbor.

Platform Description

N/A

5.30 ip ospf message-digest-key

Use this command to configure the MD5 authentication key in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf message-digest-key *key-id* **md5** [**0 | 7**] *key*

no ip ospf message-digest-key *key-id*

Parameter Description

Parameter	Description
key	Key of up to 16 characters
0	Displays the key in plain text.
7	Displays the key in cipher text.
key-id	Key identifier in the range from1 to 255

Defaults

No MD5 key is configured by default.

Command Mode

Interface configuration mode

Usage Guide

The **ip ospf message-digest-key** command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighboring relationship cannot be established between two devices directly connected, and thus route information exchange is impossible.

The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key. For neighbors, the same key identifier must correspond to the same key.

To enable OSPF area authentication, execute the **area authentication** command in routing process configuration mode. The authentication can be enabled separately on an interface by executing the **ip ospf authentication** command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.

The FSOS software supports smooth modification of MD5 authentication keys, which shall be added before deleted. When an MD5 authentication key of the device is added, the device will regard other devices have not had new keys and thus send multiple OSPF packets by using different keys, till it confirms that the neighbors have been configured with new keys. When all devices have been configured with new keys, it is possible to delete the old key.

Configuration Examples

The following example adds a new OSPF authentication key "hello5" with key ID 5 for fastEthernet 0/1.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip address 172.16.24.2 255.255.255.0
FS(config-if-FastEthernet 0/1)# ip ospf authentication message-digest
FS(config-if-FastEthernet 0/1)# ip ospf message-digest-key 10 md5 hello10
FS(config-if-FastEthernet 0/1)# ip ospf message-digest-key 5md5 hello5
```

When all neighbors are added with new keys, the old keys shall be deleted for all devices.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# no ip ospf message-digest-key10md5 hello10
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication and defines authentication mode.
ip ospf authentication	Enables authentication on the interface and defines authentication mode.

Platform Description

N/A

5.31 ip ospf mtu-ignore

Use this command to disable the MTU check when an interface receives the database description packet. Use the **no** form of this command to restore the default setting.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults

MTU check is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

After receiving the database description packet, the device will check whether the MTU of the neighbor interface is the same as its own MTU. If the received database description packet indicates an MTU greater than the interface's MTU, the neighboring relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration Examples

The following example disables the MTU check function on fastEthernet 0/1.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip ospf mtu-ignore
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.32 ip ospf network

Use this command to configure the OSPF network type in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf network { **broadcast** | **non-broadcast** |
point-to-multipoint [**non-broadcast**] | **point-to-point** }
no ip ospf network

Parameter Description

Parameter	Description
broadcast	Sets the OSPF network type as the broadcast type.
non-broadcast	Sets the OSPF network type as the non-broadcast multi-path access type, i.e. NBMA network.
point-to-multipoint [non-broadcast]	Sets the OSPF network type as the point-to-multipoint type. The value is the point-to-multipoint broadcast type by default. The non-broadcast option means the point-to-multipoint non-broadcast type.
point-to-point	Sets the OSPF network type as the point-to-point type.

Defaults

The default configurations are as follows:

PTP network type: Point-to-Point Protocol(PPP), Serial Line Internet Protocol(SLIP), frame relay point-to-point (PTP) sub-interface, X.25 PTP sub-interface encapsulation

NBMA network type: frame relay (except for PTP sub-interface), X.25 encapsulation (except for PTP sub-interface)

Broadcast network type: Ethernet encapsulation

By default, the network type is the point-to-multipoint network type.

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.

Configuration Examples

The following example configures the frame relay interface network as the P2P type.

```
FS(config)# interface Serial 1/0
FS(config-Serial 1/0)#ip address 172.16.24.4 255.255.255.0
FS(config-Serial 1/0)# encapsulation frame-relay
FS(config-Serial 1/0)# ip ospf network point-to-point
```

The following example configures the frame relay interface network as the NBMA type.

```
FS(config)# interface Serial 1/0
FS(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0
FS(config-Serial 1/0)# encapsulation frame-relay
FS(config-Serial 1/0)# ip ospf network non-broadcast
FS(config-Serial 1/0)#exit
FS(config)# router ospf 20
FS(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related Commands

Command	Description
dialer map ip	Defines the mapping between IP address and dialing number.
frame-relay map	Defines the mapping between IP address and frame DLCI.
neighbor(OSPF)	Defines the IP address of neighbor applicable to NBMA network type and point-to-multipoint non-broadcast type only.
X25 map	Defines the mapping between IP address and X.25 network address.

Platform Description

N/A

5.33 ip ospf priority

Use this command to configure the OSPF priority in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf priority *priority*

no ip ospf priority

Parameter Description

Parameter	Description
priority	Sets the OSPF priority of the interface in the range from 0 to 255.

Defaults

The default is 1.

Command Mode

Interface configuration mode

Usage Guide

The interface priority is included in the Hello packet. When DR/BDR election occurs in the OSPF broadcast type network, the device with higher priority will become the DR or BDR. If the devices have the same priority, the one with higher ID will become the DR or BDR. The device with priority 0 cannot become DR or BDR. This command is valid only for OSPF broadcast and non-broadcast network types.

Configuration Examples

The following example configures the priority offastethernet 0/1 as 0.

```
Switch(config)#interface fastethernet 0/1
FS(config-if-FastEthernet 0/1)# ipospfpriority0
```

Related Commands

Command	Description
ip ospf network	Configures the network type of the interface.

Platform Description

N/A

5.34 ip ospf retransmit-interval

Use this command to define the interval for sending the link state update (LSU) packet on the interface in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf retransmit-interval *seconds*

ip ospf retransmit-interval

Parameter Description

Parameter	Description
seconds	Interval for sending the LSU packets in seconds. The range is from 0 to 65535. This interval must be greater than the round trip delay of packets between two neighbors.

Defaults

The default is 5.

Command Mode

Interface configuration mode

Usage Guide

After the device sends an LSU packet, the LSU packet stays in the transmission buffer queue. If no confirmation from the neighbor is obtained in the interval defined with the **ip ospf retransmit-interval** command, the LSU will be sent once again.

In serial lines or virtual links, the retransmission interval shall be slightly larger. The LSU packet retransmission interval of virtual links is defined with the area virtual-link command followed with the keyword retransmit-interval.

Configuration Examples

The following example configures the LSU packet retransmission interval on fastEthernet 0/1 as 10 seconds.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip ospf retransmit-interval 10
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform Description

N/A

5.35 ip ospf source-check-ignore

Use this command to disable the source address check in the point-to-point link. Use the **no** form of this command to restore the default setting

ip ospf source-check-ignore

no ip ospf source-check-ignore

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Interface configuration mode

Usage Guide

For OSPF, the source address of the received packet is required to be in the same network segment with the receiving interface. However, in a point-to-point link, the addresses of two ends of the link are individually set, and they are not required to be in the same network segment. The peer address is informed during the process of point-to-point link negotiation; therefore, OSPF will check whether the source address of the packet is the informed one. If no, the OSPF regards this packet as illegal and drops it. In some applications, the addresses informed during the negotiation are shielded. You need to disable the source address check to ensure the normal establishment of OSPF neighbors. The source address check shall be never enabled, especially for the unnumbered interfaces.

Configuration Examples

The following example disables the source address check function in the point-to-point link.

```
FS(config)# interface serial 1/0
FS(config-if)# ip ospf source-check-ignore
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

5.36 ip ospf transmit-delay

Use this command to define the LSU packet transmission delay in interface configuration mode. Use the **no** form of this command to restore the default setting.

ip ospf transmit delay *seconds*

no ip ospf transmit delay

Parameter Description

Parameter	Description
seconds	LSU packet transmission delay in seconds in the range from 1 to 65535.

Defaults The default is 1.

Command Mode Interface configuration mode

Usage Guide Before the LSU packet is transmitted, the Age field in all the LSAs of the packet will be increased by the value defined with the **ip ospf transmit-delay** command in interface configuration mode. The configuration of this parameter shall consider the transmission and line transmission delay of the interface. For low-rate lines, the transmission delay of the interface shall be slightly larger. The LSU packet transmission delay of the virtual link is defined with the **area virtual-link** command followed with the keyword retransmit-interval.

The FSOS software will resend or request resending the LSA with Age up to 3600. If no update is obtained in time, the aged LSA will be cleared from the link state database.

Configuration Examples The following example configures the transmission delay of fastEthernet 0/1 as 10.

```
FS(config)# interface fastEthernet 0/1
FS(config-if-FastEthernet 0/1)# ip ospf transmit-delay 10
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

Platform Description N/A

5.37 log-adj-changes

Use this command to enable the logging of the neighbor state changes. Use the **no** form of the command to disable this function.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Parameter Description

Parameter	Description
detail	Records the detail of changes.

Defaults This function is enabled by default. Without the detail parameter, the system records the logs that the neighbor enters or exits the full state.

Command Mode Routing process configuration mode

Usage Guide N/A

Configuration Examples The following example logs the neighbor state changes.

```
FS(config)# router ospf 1
FS(config-router)# log-adj-changes detail
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF global configuration information.

Platform Description N/A

5.38 max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum number of DD packets in the range from1 to 65535

Defaults The default is 5.

Command Mode Routing process configuration mode

Usage Guide When a router is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have at the same time.

Configuration Examples

The following example sets the maximum number of DD packets to 4.

After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
FS(config)# routerospf10
FS(config-router)# max-concurrent-dd4
```

Related Commands

Command	Description
router ospf max-concurrent-dd	Sets the maximum number of neighbors allowed in concurrent interaction for all OSPF routing processes.

Platform Description

N/A

5.39 max-metric

Use this command to set the maximum metric of the router-lsa, so that this routing device will not firstly be used as the transmission node by other devices in SPF computing. Use the **no** form of this command to restore the default setting.

max-metric router-lsa [external-lsa *[max-metric-value]]* [**include-stub**] [**on-startup** *[seconds]]* [**summary-lsa** *[max-metric-value]]*

no max-metric router-lsa [external-lsa *[max-metric-value]]* [**include-stub**] [**on-startup** *[seconds]]* [**summary-lsa** *[max-metric-value]]*

Parameter Description

Parameter	Description
router-lsa	Configures the maximum metric (0XFFFF) of non-stub links in the Router LSA.
external-lsa	Uses the maximum metric instead of the external-lsa metric (including the Type-5 and Type-7).
max-metric-value	Maximum metric of the LAS. The range is 1 to 16777215.The default value is 16711680,
include-stub	Configures the maximum metric of the stub links in the Router LSA.
on-startup	Advertises the maximum metric when the routing device starts up.
seconds	Interval of advertising the maximum metric. The range is 5 to 86400. The default value is 600 seconds.
summary-lsa	Uses the maximum metric to replace the summary LSA metric. (including Type-3 and Type-4)

Defaults

The normal metric LSAs are used by default.

Command Mode

Routing process configuration mode

Usage Guide

With the **max-metric router-lsa** command enabled, the maximum metric of non-stub links in the Router LSA generated by the routing device is set. The link's normal metric is restored after canceling this configuration or reaching the timer.

By default, with this command enabled, the normal metric of the stub links is still advertised, which is the output interface cost. If the **include-stub** parameter is configured, the maximum metric of the stub links will be advertised.

When the device acts as an ABR, if no interval flow transmission is expected, use the **summary-lsa** parameter to set the summary LSA as the maximum metric.

When the device acts as an ASBR device, if no external flow transmission is expected, use the **external lsa** parameter to set the external LSA as the maximum metric.

The **max-metric router-lsa** command is usually used in the following scenes:

The device is restarted, which generally makes the IGP protocol converge faster, so that other devices attempt forwarding the dataflow through the new started-up device.

The device is added into the network without being used for dataflow transmission. If the backup path exists, the current device is not used for the dataflow transmission. Otherwise, this device is still used to transmit the dataflow.

Remove the device from the network gracefully. With this command enabled, the current device advertises the maximum metric to all devices, as that the other devices in this network can choose the backup path to for the dataflow transmission before the current device is removed.

For the OSPF implementation in the earlier versions (RFC 1247 or earlier versions), the links with the maximum metric (0xFFFF) in the LSA will not participate in the SPF calculation, that is, no dataflow will be sent to the router that have generated these LSAs.

Configuration Examples

The following example configures the LSA maximum metric as 100 seconds after starting the device.

```
FS(config)# router ospf 20
FS(config-router)# max-metric router-lsa on-startup 100
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF related configurations.

Platform Description

N/A

5.40 neighbor

Use this command to define the OSPF neighbor in routing process configuration mode. Use the **no** form of this command to restore the default setting.

Neighbor *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost*]]

no neighbor *ip-address* [[**poll-interval**] [**priority**] | [cost]]

Parameter Description

Parameter	Description
ip address	IP address of the neighbor
poll-interval *seconds*	(Optional) Specifies the interval of polling neighbors in seconds. The range is

	from 0 to 2147483647. Only the non-broadcast (NBMA) network type supports this option.
priority *priority*	(Optional) Configures the priority of non-broadcast network neighbors. The range is from 0 to 255. Only the non-broadcast (NBMA) network type supports this option.
cost *cost*	(Optional) Configures the cost to each neighbor in point-to-multipoint network, not defined by default, where the cost configured on the interface will be used. The range is from 0 to 65535. Only the point-to-multipoint [non-broadcast] network type supports this option.

Defaults

No neighbor is defined by default.

The default neighbor polling interval is 120 seconds.

The default NBMA neighbor priority is 0.

Command Mode

Routing process configuration mode

Usage Guide

The FSOS software must explicitly configure the neighbor information for every non-broadcast network neighbor. The IP address of a neighbor must be the master IP address of that neighbor interface.

In the NBMA network, if the neighbor device becomes inactive, in other words, if the Hello packet is not received within the device dead-interval, the OSPF will send more Hello packets to the neighbor. The interval at which the Hello packets are sent is called the polling interval. When the OSPF starts to work for the first time, it sends Hello packets only to the neighbor whose priority is not 0, so that the neighbor whose priority is set as 0 will not participate in the DR/BDR election. When the DR/BDR is generated, the DR/BDR sends the Hello packets to all neighbors to establish the neighbor relationship.

Since the point-to-multipoint non-broadcast network has no broadcast capability, neighbors cannot be found dynamically. So, it is required to use this command to manually configure neighbor. In addition, it is possible to configure the cost to each neighbor through the cost option for the point-to-multipoint network type.

Configuration Examples

The following example declares an OSPF non-broadcast network neighbor, with the IP address 172.16.24.2, priority 1 and polling interval 150 seconds.

```
FS(config)# routerospf 20
FS(config-router)# network 172.16.24.0 0.0.0.255 area 0
FS(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

Related Commands

Command	Description
ip ospf priority	Sets the interface priority.
ip ospf network	Sets the network type

Platform Description

N/A

5.41 network area

Use this command to define which interfaces run OSPF and the OSPF areas they belong to in routing process configuration mode. Use the **no** form of this command to restore the default setting.

network *ip-address wildcard* **area** *area-id*

no network *ip-address wildcard* **area** *area-id*

Parameter Description

Parameter	Description
ip-address	IP address of the interface
wildcard	Defines the comparison bits in the IP address, with 0 for exact match and 1 for no comparison
area-id	OSPF area identifier. An OSPF area is always associated with an address range. For easy of management, a subnet can be used as the OSPF area identifier.

Defaults

No OSPF area is configured by default.

Command Mode

Routing process configuration mode

Usage Guide

The ip-address and wildcard parameters allow associating multiple interfaces with one OSPF area. To run OSPF on an interface, it is required to include the primary IP address and secondary IP address of the interface in the IP address range defined by the network area command. If only the secondary IP address is included, OSPF cannot be enabled on the interface.

You can determine the OSPF process that the interface takes part in by the means of the best match if the IP address of the interface matches the IP address ranges defined by the network command in multiple OSPF processes.

Configuration Examples

The following example defines:

Three areas: 0, 1 and 172.16.16.0

The interfaces whose IP addresses fall into the 192.168.12.0/24 range to area 1

The interfaces whose IP addresses fall into the 172.16.16.0/20 range to area 2

The remaining interface being assigned to area 0.

```
FS(config)# routerospf 20
FS(config-router)# network172.16.16.0
0.0.15.255 area172.16.16.0
FS(config-router)# network192.168.12.0
0.0.0.255 area 1
FS(config-router)# network0.0.0.0 255.255.255.255 area0
```

Related Commands

Command	Description
router ospf	Creates the OSPF routing process.

Platform Description N/A

5.42 overflow database

Use this command to configure the maximum number of LSAs supported by the current OSPF instance. Use the **no** form of this command to restore the default setting.

overflow database *number* [**hard | soft**]

no overflow database

Parameter Description

Parameter	Description
number	Maximum number of LSAs. The range is from 1 to 4294967294.
hard | soft	hard: shuts down the OSPF instance when the number of LSAs exceeds that number. soft: issues an alarm when the number of LSAs exceeds that number.

Defaults The maximum number of LSAs supported by the current OSPF instance is not restricted by default.

Command Mode Routing process configuration mode

Usage Guide To shut down the OSPF instance when the number of LSAs exceeds that number, use the hard parameter; otherwise, use the soft parameter.

Configuration Examples The following example configures that OSPF instance 10 will be shut down when there are more than 10 LSAs.

```
FS(config)# router ospf 10
FS(config-router)# overflow database 10 hard
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.43 overflow database external

Use this command to configure the maximum number of external LSAs and the waiting time from the overflow state to the normal state. Use the **no** form of this command to restore the default setting.

overflow database external *max-dbsize wait-time*

no overflow database external

Parameter Description

Parameter	Description

max-dbsize	Maximum number of external LSAs (the value shall be the same for all routing devices in the same AS). The range is from 0 to 2147483647.
wait-time	Waiting time of the routing device from the overflow status to normal status. The range is from 0 to 2147483647.

Defaults

The maximum number of external-LSAs is not restricted by default.

If the maximum number of external-LSAs is restricted, the normal status cannot be restored when the maximum number is exceeded.

Command Mode

Routing process configuration mode

Usage Guide

When the number of external-LSAs exceeds the value of max-db size, the device enters the overflow state. Then no more external-LSA will be loaded and the external-LSAs generated locally will be cleared. After wait-time expires, the device restores to the normal state and external-LSAs are reloaded.

⚠ When using this function, ensure that all routers of the OSPF backbone area and common areas use the same max-db size value. Otherwise, the following situations occur:

⚠ The link status is inconsistent on the entire network and neighbors fail to achieve the Full state.

⚠ Incorrect routes occur, including loops.

⚠ AS-External-LSAs may be frequently retransmitted.

Configuration Examples

The following example configures that the maximum number of external LSAs is 10, and it turns to the overflow status upon timeout, and the time interval attempting to restore from the overflow state to the normal state is 3 seconds.

```
FS(config)# routerospf10
FS(config-router)# overflow database external10 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.44 overflow memory-lack

Use this command to allow OSPF to enter the OVERFLOW state when the memory lacks. Use the **no** form of this command to disable this function.

overflow memory-lack

no overflow memory-lack

Parameter Description

Parameter	Description

N/A	N/A

Defaults This function is enabled by default

Command Mode Routing process configuration mode

Usage Guide The action of OSPF entering the OVERFLOW state is to discard the newly-learned external route and effectively prevent the memory from increasing.

It is possible that enabling this function causes the route loop in the whole network. To reduce that possibility, OSPF will generate a default route directing to the NULL port and this default route will exist in the OVERFLOW state.

Use the **clear ip ospf process** command to reset the OSPF and remove the OSPF OVERFLOW state.

Use the no form of this command to prevent the OSPF to enter the OVERFLOW state when the memory is insufficient, which may result in the constantly consumption of the memory resources. If the memory is exhausted to some degree, the OSPF instance will stop and all learned routes will be removed.

Configuration Examples The following example prevents the OSPF from entering the OVERFLOW state when the memory is insufficient.

```
FS(config)# router ospf 1
FS(config-router)# no overflow memory-lack
```

Related Commands

Command	Description
clear ip ospf process	Resets the OSPF instances.
show ip protocols ospf	Displays the OSPF information.

Platform Description N/A

5.45 passive-interface

Use this command to configure the specified network interface or all interface as the passive interfaces. Use the **no** form of this command to restore the default setting.

passive-interface { **default |** *interface-type interface-number* | *interface-type interface-number ip-address* }

no passive-interface { **default |** *interface-type interface-number* | *interface-type interface-number ip-address* }

Parameter Description

Parameter	Description
interface-type interface-number	Interface to be set as a passive interface
default	Sets all the interfaces as passive interfaces
interface-type interface-number ip-address	Sets the address of the specified interface as a passive address.

Defaults No interface is configured as a passive interface by default. All interfaces are allowed to receive or send OSPF packets.

Command Mode Routing process configuration mode

Usage Guide To prevent other devices in the network from dynamically learning the routing information of the device, set the specified network interface of this device as a passive interface or the IP address of the specified network interface as a passive address

Configuration Examples The following example configures fastEthernet 0/1 as a passive interface and the IP address of the interface 1.1.1.1 as the passive address.

```
FS(config)# routerospf 30
FS(config-router)# passive-interface fastEthernet 0/1
FS(config-router)# passive-interface fastEthernet 0/1 1.1.1.1
```

Related Commands

Command	Description
show ip ospf interface	Displays the configuration information of the interface.

Platform Description N/A

5.46 redistribute

Use this command to redistribute the external routing information. Use the **no** form of this command to restore the default setting.

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*]

no redistribute { **connected** | **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*] [**subnets**] [**tag** *tag-value*]

Parameter Description

Parameter	Description
connected	Redistribution from direct routes
ospf *process-id*	Redistribution from an ospf instance specified in process-id in the range from 1 to 65,535
rip	Redistribution from rip
static	Redistribution from static routes
match	Filters specified routes for configuring OSPF route redistribution. By default, all the OSPF routes are redistributed.
metric *metric-value*	Specifies the metric of an OSPF external LSA in the range from 0 to 16777214.
metric-type{1|2}	Sets the external routing type as E-1 or E-2.

route-map *route-map-name*	Redistribution filter rule
subnets	Redistributes the routes of non standard networks.
tag *tag-value*	Sets the tag value of the routes redistributed to the OSPF in the range from 0 to 4294967295.

Defaults

Redistribution configuration is not supported by default.

If you configure OSPF redistribution, all subtype routes of the instance are redistributed.

In other cases, all routings of this type are redistributed.

The default value of metric-type is E-2.

No route-map is associated by default.

Command Mode

Route configuration mode

Usage Guide

After the command is configured, the router will become an ASBR, and the related routing information is imported into the OSPF domain and broadcasted to other OSPF routers through type-5 LSAs.

When you configure OSPF router distribution without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. Use the no form of this command to restore the default configuration.

ⓘ The range of set metric is from 0 to 16777214 for the associated route-map. If the value exceeds the range, introducing a route fails. The following are the rules for configuring the no form of the redistribute command.1. If the **no** form specifies some parameters, restore their default values.

ⓘ 2. If the **no** form contains no parameter, delete the whole command.

Configuration Examples

Related Commands

Command	Description
summary-address	Configures the aggregate route for the external route of the OSPF route area.
default-metric	Sets the default metric of the OSPF redistribution route.

Platform Description

N/A

5.47 router ospf

Use this command to create the OSPF routing process in global configuration mode. Use the **no** form of this command to restore the default setting.

router ospf

Parameter Description

Parameter	Description
N/A	N/A

Defaults No OSPF routing process exists by default.

Command Mode Global configuration mode

Usage Guide Based on the original implementation, the FSOS10.1 adds the routing process ID to multi-instance OSPF. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols that run independently.

Configuration Examples

```
N/A
```

Related Commands

Command	Description
show ip protocols	Displays the routing protocol information.
show ip ospf	Displays the OSPF information.

Platform Description N/A

5.48 router ospf max-concurrent-dd

Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the **no** form of this command to restore the default setting.

router ospf max-concurrent-dd *number*

no router ospf max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum number of DD packets in the range from 1 to 65535.

Defaults The default is 10.

Command Mode Global configuration mode

Usage Guide When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have (initiated or accepted) at the same time.

Configuration Examples

The following example sets the maximum number of DD packets to 4.

After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors.

```
FS# configure terminal
FS(config)# router ospfmax-concurrent-dd4
```

Related Commands

Command	Description
max-concurrent-dd	Sets the maximum number of the neighbors that the OSPF routing process can concurrently interact with.

Platform Description

N/A

5.49 router-id

Use this command to set the router ID. Use the **no** form of this command to restore the default setting.

router-id *router-id*

no router-id

Parameter Description

Parameter	Description
router-id	Router ID in IP address form

Defaults

The OSPF routing process will select the maximal interface IP address as the router ID by default.

If the loopback interface of an IP address is not configured, the OSPF routing process will select the maximum IP address among all its physical interfaces as the router ID.

Command Mode

Routing process configuration mode

Usage Guide

You can configure any IP address as the router ID. However, the router ID should be unique. Note that once the router ID changes, the OSPF protocol will do a lot of processing. Therefore, it is not recommended to change the router ID. The device can be changed only when no LSA is generated.

Configuration Examples

The following example modifies the router ID to 0.0.0.36.

```
FS(config)# router ospf 20
FS(config-router)# router-id0.0.0.36
```

Related Commands

Command	Description
show ip protocols	Displays the routing protocol information.

Platform Description N/A

5.50 show ip ospf

Use this command to display the OSPF information.

show ip ospf [*process-id*]

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the information of the OSPF routing process.

Configuration Examples The following example displays the output of the **show ip ospf** command.

```
FS# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Domain ID type 0x0105, value 0x010101010101
Process uptime is 4 minutes
Process bound to VRF default
Memory Overflow is enabled.
Router is not in overflow state now.
Conforms to RFC2328, and RFC1583Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Enable two-way-maintain
Supports opaque LSA
Supports Graceful Restart
This router is an ASBR (injecting external routing information)
Originating router-LSAs with maximum metric
Condition:on startup for 100 seconds, State:inactive
Advertise stub links with maximum metric in router-LSAs
Advertise summary-LSAs with metric 16711680
Advertise external-LSAs with metric 16711680
Unset reason:timer expired, Originated for 100 seconds
Unset time:00:02:02.080, Time elapsed: 00:23:54.656
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
```

```
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 10 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group:240 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes :Enabled
Graceful-restart disabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
BFD enabled
Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
Number of LSA 3. Checksum 0x0204bf
Area 1 (NSSA)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 0
Number of fully adjacent virtual neighbors through this area is 0
Area has no authentication
SPF algorithm last executed 02:09:23.040 ago
SPF algorithm executed 4 times
Number of LSA 6. Checksum 0x028638
NSSA Translator State is disabled, Stability Interval expired in 00:00:03
```

Field	Description
Router ID	ID of a router.
Process uptime	Effective time of the current OSPF process (the process does not take effect when device-id is 0.0.0.0)
Bou to VRF	VRF of the current OSPF
Conforms to RFC2328	Same as the RFC2328

RFC1583Compatibilit flag	Whether the RFC1583 or RFC2328 is adopted for the calculation of external routes. This policy is used in the selection of best ASBR and in the route comparison.
Support Tos	Supports Only TOS0.
Supports opaque LSA	Supports opaque-LSA.
Graceful-restart	GR Restart capability described in the RFC3623 Graceful Restart
Graceful-restart helper	GR Help capability described in the RFC3623 Graceful Restart
Router Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	Parameter used for LSA pacing, checksum calculation, and aging interval
Incomming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.
Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated

Number of LSA received	Number of LSAs received
Log Neighbor Adjency Changes	Whether the record switch for neighbor status change is enabled
Number of areas attached to this router	Total number of areas on the devices
Area type	Area type, including normal, stub, and nssa
Number of interfaces in this area	Number of interfaces in this area
Number of fully adjacent neighbors in this area	Number of Full neighbors of the area
Number of fully adjacent virtual neighbors through this area	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area
NSSATranslatorState	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA.
BFD enabled	Enables BFD for OSPF.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.51 show ip ospf border-routers

Use this command to display the OSPF internal routing table on the ABR/ASBR.

show ip ospf [*process-id*] **border-routers**

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the OSPF internal routes from the local routing device to the ABR or ASBR. The OSPF internal routing table is different from the one displayed with the show ip route command. The OSPF internal routing table has the destination address of the router ID instead of the destination network.

Configuration Examples The following example displays the output of the **show ip ospf border-mrouters** command.

```
FS# show ip ospf border-routers
OSPF internal Routing Table
Codes:i - Intra-area route, I - Inter-area route
i 1.1.1.1 [2] via 10.0.0.1, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select
```

The following table describes fields in the output.

Field	Description
Codes	Route type code, where “i” means intra-area routes, while “I” means inter-area routes.
I	Intra-area routes
1.1.1.1	Displays the OSPF ID of the border device.
[2]	Displays the cost to the border device.
via 10.0.0.1	Displays the next-hop gateway to the border device.
FastEthernet 0/1	Displays the interface to the border device.
ABR, ASBR	Displays the type of the border device, including ABR, ASBR, or both.
Area 0.0.0.1	Displays the area that learns the route.
select	Indicates the currently selected optimal path when there are multiple paths to the ASBR.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.52 show ip ospf database

Use this command to display the OSPF link state database information. Use the **no** form of this command to restore the default setting. Different formats of the command will display different LSA information.

show ip ospf [*process-id* [*area-id* | *ip-address*]] **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**]

Parameter Description

Parameter	Description
area-id	(Optional) Displays the area ID.
adv-device	(Optional) Displays the LSA information generated by the specified advertising device.
link-state-id	(Optional) Displays the LSA information of the specified OSPF link state identifier.
self-originate	(Optional) Displays the LSA information generated by the device itself.
Max-age	(Optional) Displays the LSAs aged.
router	(Optional) Displays the OSPF device LSA information.
network	(Optional) Displays the OSPF network LSA information.
summary	(Optional) Displays the OSPF summary LSA information.
asbr-summary	(Optional) Displays the ASBR summary LSA information.
external	(Optional) Displays the OSPF external LSA information.
nssa-external	(Optional) Displays the category 7 OSPF external LSA information.
opaque-area	(Optional) Displays type 10 LSAs.
opaque-as	(Optional) Displays type 11 LSAs.
opaque-link	(Optional) Displays type 9 LSAs.
database-summary	(Optional) Displays the statistics of LSAs of the link state database.
detail	Displays detailed information of LSAs of the OSPF.
brief	Displays the brief information of the LSAs of the specified type.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

When the OSPF link state database is very large, you should display the information on the link state database by item. Proper use of commands may help OSPF troubleshooting.

Configuration Examples

The following example displays the output of the **show ip ospf database** command.

```
FS# show ip ospf database
OSPF Device with ID (1.1.1.1) (Process ID 1)
Device Link States (Area 0.0.0.0)
Link ID          ADV Device        Age   Seq#          CkSum    Link count
1.1.1.1          1.1.1.1           2     0x80000011 0x6f39 2
3.3.3.3          3.3.3.3           120   0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
Link ID          ADV Device        Age   Seq#          CkSum
192.88.88.27     1.1.1.1           120   0x80000001 0x5366
```

```
Summary Link States (Area 0.0.0.0)
Link ID          ADV Device       Age   Seq#          CkSum    Route
10.0.0.0         1.1.1.1          2     0x80000003 0x350d 10.0.0.0/24
100.0.0.0        1.1.1.1          2     0x8000000c 0x1ecb 100.0.0.0/16
Device Link States (Area 0.0.0.1 [NSSA])
Link ID          ADV Device       Age   Seq#          CkSum    Link count
1.1.1.1          1.1.1.1          2     0x80000001 0x91a2 1
            Summary Link States (Area 0.0.0.1 [NSSA])
Link ID          ADV Device       Age   Seq#          CkSum    Route
100.0.0.0        1.1.1.1          2     0x80000001 0x52a4 100.0.0.0/16
192.88.88.0      1.1.1.1          2     0x80000001 0xbb2d 192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID          ADV Device       Age   Seq#          CkSum    Route                Tag
20.0.0.0         1.1.1.1          1     0x80000001 0x033c E2 20.0.0.0/24     0
100.0.0.0        1.1.1.1          1     0x80000001 0x9469 E2 100.0.0.0/28    0
AS External Link States
Link ID          ADV Device       Age   Seq#          CkSum    Route                Tag
20.0.0.0         1.1.1.1          380   0x8000000a 0x7627 E2 20.0.0.0/24     0
100.0.0.0        1.1.1.1          620   0x8000000a 0x0854 E2 100.0.0.0/28    0
```

The following table describes the fields in the output of the **show ip ospf database** command.

Field	Description
OSPF Device with ID	Displays the Router ID.
Device Link States	Displays the device LSA information.
Net Link States	Displays the network LSA information.
Summary Net Link States	Displays the summary network LSA information.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
AS External Link States	Displays the type 5 autonomous external LSA information.
Link ID	Displays the Link ID.
ADV Device	Displays the ID of the device that advertises the LSAs.
Age	Displays the keepalive period of the LSA.
Seq#	Displays the sequence number of the LSA, which is used to check aged or duplicate LSAs.
Cksum	Displays the checksum of LSAs.
Link-Count	Displays the number of links in the device LSA information.
Route	Displays the device information included in the LSA.
Tag	Displays the tag of the LSA.

The following example displays the output the **show ip ospf database asbr-summary** command.

```
FS# show ip ospf database asbr-summary
```

```
        OSPF Device with ID (1.1.1.35) (Process ID 1)
              ASBR-Summary Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: ASBR-summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Device address)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
        TOS: 0     Metric: 1
```

The following table describes the fields in the output of the **show ip ospf database asbr-summary** command.

Field	Description
OSPF Device with ID	Displays the router ID.
AS Summary Link States	Displays the summary LSA information in the AS.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
AdvertisingRouter	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be only 0 now.
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database external** command.

```
FS# show ip ospf database external
        OSPF Device with ID (1.1.1.35) (Process ID 1)
              AS External Link States
LS age: 752
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-5 AS External Link States	Displays autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Indicates the external link type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used by other routing processes to redistribute OSPF routes.

The following example displays the output of the **show ip ospf database network** command:

```
FS# show ip ospf database network
OSPF Router with ID (1.1.1.1) (Process ID 1)
Network Link States (Area 0.0.0.0)
LS age: 572
Options:0x2 (*|-|-|-|-|-|E|-)
LS Type:network-LSA
Link State ID:192.88.88.27 (address of Designated Router)
Advertising Router:1.1.1.1
LS Seq Number: 80000001
Checksum:0x5366
Length: 32
Network Mask: /24
```

```
Attached Router:1.1.1.1
Attached Router:3.3.3.3
```

The following table describes the fields in the output of the **show ip ospf database network** command.

Field	Description
OSPF Router with ID	Displays the router ID corresponding to the follow-up information and the process ID corresponding to the OSPF.
Network LinStates	Displays the network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Device	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the network corresponding to the LSA.
Attached Router	Displays the device that is connected with the network.

The following example displays the output of the **show ip ospf database device** command:

```
FS# show ip ospf database router
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
LS age: 322
Options:0x2 (*|-|-|-|-|-|E|-)
Flags:0x3 :ABR ASBR
LS Type:router-LSA
Link State ID:1.1.1.1
Advertising Router:1.1.1.1
LS Seq Number: 80000012
Checksum:0x6d3a
Length: 48
Number of Links: 2
Link connected to:Stub Network
(Link ID) Network/subnet number: 100.0.1.1
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metric: 0
```

The following table describes the fields in the output of the **show ip ospf database device** command.

Field	Description
OSPF Device with ID	Displays the router ID.

Device Link States	Displays the device LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
Flag	Flag
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Number of Links	Displays the number of links associated with the device.
Link connected to	Displays what the link is connected to and the network type.
(Link ID)	Link identifier
(Link Data)	Link data
Number of TOS metrics	TOS value, supporting TOS0 only
TOS 0 Metrics	TOS0 metric

The following example displays the output of the **show ip ospf database summary** command:

```
FS# show ip ospf database summary
            OSPF Device with ID (1.1.1.1) (Process ID 1)
                    Summary Link States (Area 0.0.0.0)
LS age: 499
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.0.0.0 (summary Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x330e
Length: 28
Network Mask: /24
            TOS: 0     Metric: 11
```

The following table describes the fields in the output of the **show ip ospf database summary** command.

Field	Description
OSPF Router with ID	Displays the router ID.
Summary Net Link States	Displays the summary network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, supporting only 0 now
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database nssa-external** command:

```
FS# show ip ospf database nssa-external
            OSPF Device with ID (1.1.1.1) (Process ID 1)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 1
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x033c
Length: 36
Network Mask: /24
            Metric Type: 2 (Larger than any link state path)
            TOS: 0
            Metric: 20
            NSSA: Forward Address: 100.0.2.1
            External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database nssa-external** command.

Field	Description
OSPF Router with ID	Displays the router ID.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequential number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
NSSA:Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database external** command:

```
FS# show ip ospf database external
          OSPF Device with ID (1.1.1.1) (Process ID 1)
                 AS External Link States
LS age: 1290
Options: 0x2 (*|-|-|-|-|-|E|-)
```

```
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-7 AS External Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.

External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database database-summary** command:

```
FS# show ip ospf database database-summary
OSPF process 1:
Device Link States            : 4
Network Link States           : 2
Summary Link States           : 4
ASBR-Summary Link States : 0
AS External Link States    : 4
NSSA-external Link States: 2
```

The following table describes the fields in the output of the command **show ip ospf database database-summary**.

Field	Description
OSPF Process	OSPF process ID
Router Link	Number of device LSAs in the area
Network Link	Number of network LSAs in the area
Summary Link	Number of summary LSAs in the area
ASBR-Summary Link	Number of ASBR summary LSAs in the area
AS External Link	Number of NSSA LSAs in the area
NSSA-external Link	Number of NSSA LSAs in the area

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.53 show ip ospf interface

Use this command to display the OSPF-associated interface information.

show ip ospf [*process-id* **] interface [** *interface-type interface-number* **| brief]**

Parameter

Parameter	Description

Description

process-id	OSPF process ID
interface-type	(Optional) type of the specified interface
interface-number	(Optional) number of the specified interface
brief	Displays the summary of the interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the OSPF information on the interface.

Configuration Examples The following example displays the output of the **show ip ospf interface fastEthernet** *0/1* command:

```
FS# show ip ospf interface fastEthernet0/1
FastEthernet 0/1 is up, line protocol is up
Internet Address 192.88.88.27/24, Ifindex 4, Area 0.0.0.0, MTU 1500
Matching network config: 192.88.88.0/24
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1,BFD enabled
Designated Router (ID) 1.1.1.1, Interface Address 192.88.88.27
Backup Designated Router (ID) 3.3.3.3, Interface Address 192.88.88.72
Timer intervals configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:03
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 70784
Hello received 1786 sent 1787, DD received 13 sent 8
LS-Req received 2 sent 2, LS-Upd received 29 sent 53
LS-Ack received 46 sent 23, Discarded 1
```

The following table describes the fields in the output of the **show ip ospf interface serial***1/0* command.

Field	Description
FastEthernet 0/1 State	State of the network interface; UP means normal working and Down means faults.
Internet Address	Interface IP address
Area	OSPF area of the interface
MTU	Corresponding MTU
Matching network config	Network area configured for the corresponding OSPF
Process ID	Corresponding process ID
Router ID	OSPF router id
Network Type	OSPF network type
Cost	OSPF interface cost
Transmit Delay is	OSPF interface transmit delay

State	DR/BDR state ID
Priority	Priority of the interface
Designated Router(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated device(ID)	Router ID of the BRD of the interface
BDR's Interface address	Address of the BDR of the interface
Time intervals configured	Hello, Dead, Wait, and Retransmit intervals of the interface
Hello due in	Time when the previous Hello is sent
Neighbor count	Total number of neighbors
Adjacent neighbor count	Number of Full neighbors
Crypt Sequence Number	The corresponding md5 authentication number of the interface
Hello received send	Statistics on the Hello packets sent and received
DD received send	Statistics on the DD packets sent and received
LS-Req received send	Statistics on the LS request packets sent and received
LS-Upd received send	Statistics on the LS update packets sent and received
LS-Ack received send	Statistics on the LS response packets sent and received
Discard	Statistics on the discarded OSPF packets
BFD enabled	Enables BFD for OSPF.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.54 show ip ospf neighbor

Use this command to display the OSPF neighbor list.

show ip ospf [*process-id*] **neighbor**[**statistics** | { [*interface-type interface-number*] | [*neighbor-id*] | [**detail**] }]

Parameter Description

Parameter	Description
detail	(Optional) Displays the neighbor details.
interface-type interface-number	(Optional) Displays the neighbor information of the specified interface
neighbor-id	(Optional) Displays the information of the specified neighbor
statistics	(Optional) Displays the neighbor statistics.

Defaults

N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays neighbor information usually used to check whether the OSPF is running normally.

Configuration Examples The following example displays the output of the **show ip ospf neighbor** command.

```
FS# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID    Pri    State       BFD State    Dead Time    Address         Interface
3.3.3.3        1      Full/BDR    Up           00:00:32     192.88.88.72    FastEthernet 0/1

FS# show ip ospf neighbor detail
Neighbor 3.3.3.3, interface address 192.88.88.72
In the area 0.0.0.0 via interface FastEthernet 0/1
Neighbor priority is 1, State is Full, 11 state changes
DR is 192.88.88.27, BDR is 192.88.88.72
Options is 0x52 (*|O|-|EA|-|-|E|-)
Dead timer due in 00:00:32
Neighbor is up for 05:11:27
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Crypt Sequence Number is 0
Thread Inactivity Timer on
Thread Database Description Retransmission off
Thread Link State Request Retransmission off
Thread Link State Update Retransmission off
Thread Poll Timer on
Graceful-restart helper disabled
BFD session state up
```

The following table describes the fields in the output of the **show ip ospf neighbor** command.

Field	Description
Neighbor ID	Neighbor ID
Pri	Neighbor priority (for selection of DR)
State	Neighbor status
Dead Time	Remaining time for the neighbor to enter the Dead status
Address	Interface address of the neighbor
Interface	Interface of the neighbor
interface address	Interface address of the neighbor device
In the area	Displays the area that learns the neighbor.
via interface	Displays the interface that learns the neighbor

Neighbor priority	Priority of the neighbor OSPF
State	OSPF neighbor connection state. FULL means the stable state; DR indicates that the neighbor is the designated device; BDR indicates that the neighbor is the backup designated device; DROTHER indicates that the neighbor is not a DR/BDR. Point-to-point network type has no DR or DBR.
State changes times	Times of state changes
Dead Time	Dead time of the neighbor
DR	Interface address of the DR elected by the neighbor device (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected by the neighbor device (that is, the BDR field of the Hello packet)
Options	Hello packet E-bit option, where 0 indicates that the area is a STUB area; 2 indicates that the area is not a STUB area.
Dead timer due in	Dead time of the neighbor device
Neighbor up time	Period from when the device is discovered till now
Database Summary List	Statistics on the neighbor DD packets
LinkState Request List	Statistics on the neighbor LS request packets
LinkState Retransmission List	Statistics on the neighbor re-transmit packets
Crypt Sequence Number	Area MD5 authentication code
Thread Inactivity Timer	Status of invalid neighbor timer
Thread Database Description Retransmission	Status of DD packet timer of the interface
ThreadLinkState Request Retransmission	Status of LS request packet timer of the interface
ThreadLinkState Update Retransmission	Status of LS update packet timer of the interface
Thread Poll Timer	Poll Timer start status of the static neighbor
Graceful-restart helper	Whether it is able to function as the GR Helper of a specified neighbor

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.55 show ip ospf route

Use this command to display the OSPF routes.

show ip ospf [*process-id*] **route** [**count |** *ip-address mask*]

Parameter Description

Parameter	Description
process-id	OSPF process ID. All OSPF routes will be displayed without an ID specified.
count	Statistics of various OSPF routes
ip-address mask	Statistics of routes which have a specified prefix and mask.

Defaults N/A

Command Mode Privileged mode

Usage Guide This command displays the OSPF routing information. The count option displays the OSPF routing statistics.

Configuration Examples The following example displays the output of the **show ip ospf route** command.

```
OSPF process 1:
Codes: C - connected, D - Discard , 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
E2 100.0.0.0/24 [1/20] via 192.88.88.126, FastEthernet 0/1
C     192.88.88.0/24 [1] is directly connected,FastEthernet 0/1,Area 0.0.0.1
```

The following table describes the fields in the output of the **show ip ospf route** command.

Field	Description
codes	Route type and corresponding abbreviation and description
100.0.0.0/24	Route prefix
[1]	Route cost
via	Route next hop and interface

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.56 show ip ospf spf

Use this command to display the routing count in the OSPF area.

show ip ospf [*process-id*] **spf**

Parameter Description

Parameter	Description
process-id	OSPF process ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command displays the routing counts within the latest 30 minutes in the OSPF area and current routing total counts.

Configuration Examples The following example displays the output of the **show ip ospf** [*process-id*] **spf** command:

```
FS# show ip ospf 1 spf

OSPF process 1:
Area_id        30min_counts     Total_counts
0                        32                     1235
1                        6                       356
```

The following table describes the fields in the output of the **show ip ospf** [*process-id*] **spf** command.

Field	Description
Area_id	OSPF area ID
30min_counts	OSPF routing counts within the latest 30 minutes
Total_counts	Total counts of the OSPF routing till now

Related Commands

Command	Description
show ip ospf	Displays the OSPF summary.

Platform Description N/A

5.57 show ip ospf summary-address

Use this command to display the converged route of all redistributed routes.

show ip ospf [*process-id*] **summary-address**

Parameter Description

Parameter	Description
process-id	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is valid only on the NSSA ABR, and displays only the routes with local aggregation operations.

Configuration Examples The following example displays the output of the **show ip ospf summary-address** command:

```
FS# show ip ospf summary-address
OSPF Process 1, Summary-address:
172.16.0.0/16, Metric 20, Type 2, Tag 0, Match count 3, advertise
```

Field	Description
Summary Address	IP address to be aggregated
Summary Mask	Mask to be aggregated
Advertise	Whether to advertise the aggregated route
Status	Whether the aggregation range takes effect
Aggregated subnets	Number of external routes included in the aggregation range

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.58 show ip ospf virtual-link

Use this command to display the OSPF virtual link information.

show ip ospf [*process-id*] **virtual-link** [*ip-address*]

Parameter Description

Parameter	Description
process-id	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.
ip-address	Associated ID of a virtual link neighbor

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If no virtual link is configured, the command displays the neighbor status and other related information. The show ip ospf neighbor command does not display the neighbor of the virtual link.

Configuration Examples

The following is the output of the **show ip ospf virtual-links** command:

```
FS# show ip ospf virtual-links
Virtual Link VLINK0 to device 1.1.1.1 is up
Transit area 0.0.0.1 via interface FastEthernet 0/1
Local address 10.0.0.37/32
Remote address 10.0.0.27/32
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Adjacency state Full
```

The following table describes the fields in the output.

Field	Description
Virtual Link VLINK0 to router	Displays the virtual link neighbors and their status.
Virtual Link State	Displays the virtual link state.
Transit area	Displays the transit area of the virtual link.
via interface	Displays the associated interface of the virtual link.
Local address	Local interface address
Remote Address	Peer interface address
Transmit Delay	Displays the transmit delay of the virtual link.
State	Interface state
Time intervals configured	Hello, Dead, Wait, and Retransmit interval of the interface
Adjacency State	Neighbor state, where FULL means the stable state

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.59 summary-address

Use this command to configure the aggregate route out of the OSPF routing domain. Use the **no** form of this command to restore the remove the aggregate route.

summary-address *ip-address net-mask* [**not-advertise** | **tag** *value* | **cost** *cost*]

no summary-address *ip-address net-mask* [**not-advertise** | **tag** | **cost**]

Parameter Description

Parameter	Description
ip address	IP address of the aggregate route

net-mask	Network mask of the aggregate route
not-advertise	Does not advertise the aggregate route. If the parameter is not configured, the aggregate route is advertised.
tag *value*	Sets the tag value of an aggregate route. The range is from 0 to 4,294,967,295.
cost *cost*	Cost value of the aggregate route. The range is from 0 to 16,777,214.

Defaults No aggregate route is configured by default.

Command Mode Routing process configuration mode

Usage Guide When routes are redistributed by another routing process into the OSPF routing process, every route is advertised to the OSPF-enabled device separately in external LSAs. If the incoming routes are continuous addresses, the autonomous border device can advertise only one aggregate route, reducing the scale of routing table greatly.

Unlike the **area range** command, the area range command aggregates inter-OSPF-area routes, while the summary-address command aggregates external routes of the OSPF routing domain.

For the NSSA, the **summary-address** command is valid only on the NSSA ABR now, and aggregates only redistributed routes.

Configuration Examples The following example generates an external aggregate route 100.100.0.0/16.

```
FS(config)# router ospf20
FS(config-router)# summary-address100.100.0.0 255.255.0.0
FS(config-router)# redistribute static subnets
FS(config-router)# network200.2.2.0 0.0.0.255 area 1
FS(config-router)# network172.16.24.0 0.0.0.255area 0
FS(config-router)# area1nssa
```

Related Commands

Command	Description
area-range	Configures route convergence on the OSPF area border device.
redistribute	Redistributes routes of other routing processes.

Platform Description N/A

5.60 timers lsa arrival

Use this command to configure the time delay for the same LSA received. Use the **no** form of this command to restore the default setting.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter

Parameter	Description

Description

arrival-time	Configures the time delay when receiving the same LSA. The range is from 0 to 600000 in the unit of milliseconds.

Defaults The default is 1000.

Command Mode Routing process configuration mode

Usage Guide No action is done when the same LSA is received within the specified time.

Configuration Examples The following example configures the time delay for the same LSA as 2seconds.

```
FS(config)# routerospf1
FS(config-router)# timers lsa arrival 2000
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description N/A

5.61 timers pacing lsa-group

Use this command to configure the LSA grouping and then refresh the whole groups as well as the update interval for the aged link state. Use the **no** form of this command to restore the default setting.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameter Description

Parameter	Description
seconds	Parameter used for LSA pacing, checksum calculation, and aging interval. The range is from 10 to1800 in the unit of seconds.

Defaults The default is 30.

Command Mode Routing process configuration mode

Usage Guide Each LSA has its own update and aging time (LSA age). If you update and age LSAs separately, many CPU resources will be consumed. To effectively use CPU resources, you can update LSAs of a device in batches.

You can use this command to modify the value of seconds, whose default value is 240 seconds. This parameter needs not to be adjusted often. The optimal group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better.

Configuration Examples

The following example configures the pacing time as 120 seconds.

```
FS(config)# deviceospf 20
FS (config-router)# timers paing lsa-group 120
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF information.

Platform Description

N/A

5.62 timers pacing lsa-transmit

Use this command to transmit the LSA grouping updating. Use the **no** form of this command to restore the default setting.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter Description

Parameter	Description
transmit-time	Configures the interval of sending the LSA grouping. The range is from 10 to 1000.
transmit-count	Configures the number of LS-UPD packets per group. The range is from 1 to 200.

Defaults

The default configurations are as follows:

Transmit-time: 40 milliseconds.

Transmit-count: 1

Command Mode

Routing process configuration mode

Usage Guide

If there are a large number of LSAs and the load on the system is heavy, you can properly use the **transmit-time** and **transmit-count** to inhibit the flooding LS-UPD packet number in the network.

If the CPU and network bandwidth loads are not too much, reduce **transimi-time** and increase **transimit-count** to quicken the environment convergence.

Configuration Examples

The following example sets the interval of sending the LS-UPD packets as 50ms, the packets number as 20.

```
FS(config)# routerospf1
FS(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands

Command	Description
show ip ospf	Displays the OSPF process information, including the router ID.

Platform Description

N/A

5.63 timers spf

Use this command to configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations. Use the **no** form of this command to restore the default setting.

timers spf *spf-delay spf-holdtime*

no timers spf

Parameter Description

Parameter	Description
spf-delay	Defines the SPF calculation waiting period in seconds. The range is from 0 to 2147483647.After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations in seconds. The range is from 0 to 2147483647.When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start.

Defaults

For the FSOS not supporting the timers throttle spf command, the default values are as follows:

spf-delay: 5seconds;

spf-holdtime: 10 seconds.

For the FSOS supporting the timers throttle spf command, by default, the timers spf command takes no effect.

Spf-delay depends on the default configuration of the timers throttle spf command.

Command Mode

Routing process configuration mode

Usage Guide

Smaller values of *spf-delay* and *spf-holdtime* mean that OSPF adapts to the topology change faster, and the network convergence period is shorter, but this will occupy more CPU of the router.

⚠ The configurations of the **timers spf command** and the timers throttle spf command may overwrite each other.

Configuration Examples

The following example configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively.

```
FS(config)# deviceospf20
FS(config-router)# timersspf 3 9
```

Related

Command	Description

Commands

show ip ospf	Displays the configuration information of the ospf.
timers throttle spf	Configures the exponential back off delay for SPF calculation. The command is recommended to replace the timers spf command because it is more powerful.

Platform Description N/A

5.64 timers throttle lsa all

Use this command to configure the exponential back off algorithm for the LSA. Use the **no** form of this command to restore the default setting.

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description

Parameter	**Description**
delay-time	Configures the time delay of generating the LSA first. The range is from 1 to 600000.
hold-time	Configures the minimum interval of refreshing the LSA between the first time and second time. The range is from1 to 600000.
max-wait-time	Configures the maximum interval of successive refreshing the LSA., which determines whether the LSA is refreshed successively. The range is from1 to 600000

Defaults The default configurations are as follows:

Delay-time: 0 millisecond,

Hold-time: 5000 milliseconds,

Max-wait-time: 5000 milliseconds.

Command Mode Routing process configuration mode

Usage Guide If high convergence performance is required for the link change, the value of delay-time can be relatively small. if you expect to reduce the CPU consumption, increase appropriately several values.

⚠ The value of hold-time cannot be smaller than that of delay-time, and the value of max-wait-time cannot be smaller than that of hold-time.

Configuration Examples The following example configures the first delay as 10ms, hold-time as 1second and the longest delay as 5seconds.

```
FS(config)# routerospf1
FS(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the ospf

Platform Description

N/A

5.65 timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default setting.

timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

no timers throttle route { **inter-area** | **ase** }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
ia-delay	Sets the delay time of the inter-area route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the ia-delay time runs out.
ase	Calculates the external routes.
ase-delay	Defines the delay time of the external route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the ase-delay time runs out.

Defaults

The default values are as follows:

ia-delay: 0,

ase-delay: 0,

Command Mode

Routing process configuration mode

Usage Guide

The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.

Configuration Examples

The following example sets the .delay time of the inter-area route calculation to one second.

```
FS(config)# router ospf 1
FS(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.66 timers throttle spf

Use this command to configure the topology change information for OSPF, including the delay for SPF calculation as well as the interval between two SPF calculations in routing process configuration mode. Use the **no** form of this command to restore the default setting.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

Parameter	Description
spf-delay	Defines the SPF calculation waiting period, in the unit of milliseconds, in the range from1 to 600,000. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations in seconds in the range from1 to 600,000.
spf-max-waittime	Defines the maximum interval between two SPF calculations, in milliseconds in the range from1 to 60,0000.

Defaults The default configurations are as follows:

spf-delay: 1000ms;

spf-holdtime: 5000ms;

spf-max-waittime: 10000ms.

Command Mode Routing process configuration mode

Usage Guide The spf-delay parameter indicates the delay time of the topology change to the SPF calculation. The spf-holdtime parameter indicates the minimum interval between two SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval until it reaches to spf-max-waittime. If the interval between two SPF calculations has exceeded the required value, the SPF calculation will restart from spf-holdtime. Smaller spf-delay and spf-holdtime values can make the topology converge faster. A greater spf-max-waittime value can reduce the system resource consumption of SPF calculation. Those configurations can be flexibly adjusted according to the actual stability of the network topology.

Compared with the timers spf command, this command is more flexible. It speeds up the SPF calculation convergence, and reduces the system resource consumption of SPF calculation due to the topology change. To this end, the timers throttle spf command is recommended.

ℹ The value of spf-holdtime cannot be smaller than the value of spf-delay, or the value ofspf-holdtime will be set to be equal to the value of spf-delay;

The value of spf-max-waitime cannot be smaller than the value of spf-holdtime, or the value of spf-max-waittime will be set to be equal to the value of spf-holdtime automatically;

The configurations of the timers spf command and the timers throttle spf command may overwrite each other.

If both the timers spf command and the timers throttle spf command are not configured, the default value of the timers throttle spf command is used.

Configuration Examples

The following example configures the delay and holdtime and the maximum time interval of the OSPF as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the SPF calculation intervals are: 5ms, 1second, 3 seconds, 7 seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90seconds…

```
FS(config)# routerospf20
FS(config-router)# timersspf 5 1000 90000
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of OSPF
timers spf	Configures the SPF calculation delay. This command is supported in versions earlier than FSOS 10.4. It is recommended to replace the timers spf command with the timers throttle spf command.

Platform Description

N/A

5.67 two-way-maintain

Use this command to enable the OSPF two-way-maintain function. Use the **no** form of this command to disable this function.

two-way-maintain

no two-way-maintain

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

In the large-scale network, partial packets delay or dropped may exist due to much CPU and memory are occupied caused by lots of packet transmission. If the Hello packets are handled over dead-interval, the corresponding adjacency will be disconnected. In this case, you can enable the two-way-maintain function for the packets such as DD, LSU, LSR and LSAck packets from a neighbor in the network (except for the Hello packets), avoiding the neighbor invalidation caused by delayed or dropped Hello packets.

Configuration Examples

The following example disables the OSPF two-way-maintain function.

```
FS(config)# routerospf1
FS(config-router)# notwo-way-maintain
```

Related Commands

Command	Description
show ip ospf	Displays the configuration information of the OSPF

Platform Description

N/A

6 OSPFv3 Commands

6.1 area authentication

Use this command to configure OSPFv3 area authentication. Use the **no** form of this command to restore the default settings.

area *area-id* **authentication ipsec spi** *spi* [**md5** [**string-key**] **| sha1**] [**0 | 7**] *key*

no area *area-id* **authentication**

Parameter Description

Parameter	**Description**
area-id	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
md5	Specifies a message digest 5 (MD5) authentication mode.
string-key	Indicates that MD5 authentication key supports special characters.
sha1	Specifies a secure hash algorithm 1 (SHA1) authentication mode.
0	Indicates that a key is displayed in a plain-text format.
7	Indicates that a key is displayed in a cipher-text format.
key	Specifies an authentication key.

Defaults

Authentication is not performed by default.

Command Mode

Routing process configuration mode

Usage Guide

FSOS supports three authentication modes:

- null authentication mode, which is configured when authentication is not needed
- MD5 authentication mode
- SHA1 authentication mode

If OSPFv3 area authentication is configured, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Interface authentication configuration, however, takes precedence over area authentication configuration.

Configuration Examples

The following example specifies MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
FS(config-router)# area 1 authentication ipsec spi 300 md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
FS(config-router)#area 0 authentication ipsec spi 606 md5 string-key FS@123
FS(config-router)#show this

Building configuration...
!
 graceful-restart
 area 0 authentication ipsec spi 606 md5 string-key FS@123
 area 1 authentication ipsec spi 300 md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
!
end
FS(config-router)#
```

Related Commands

Command	Description
ipv6 ospf authentication	Specifies interface authentication.
area virtual-link authentication	Specifies virtual link authentication.

Platform Description

N/A

6.2 area default-cost

Use this command to set the cost of the default route for the ABR in the stub or NSSA area. Use the **no** form of this command to restore the default settings.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameter Description

Parameter	Description
area-id	Area ID of the stub or NSSA area. It can be an integer or an IPv4 prefix.
cost	Cost of the default route of the stub or NSSA area in the range from 0 to 16777215.

Defaults

The default cost is 1.

Command Mode

Routing process configuration mode.

Usage Guide

This command can only work in the ABR connected to the stub area.

Configuration Examples

The following example sets the cost of the default route of stub area 50 to 100.

```
ipv6 router ospf 1
area 50 stub
area 50 default-cost 100
```

Related Commands

Command	Description
area stub	Sets a stub area.

Platform Description N/A

6.3 area encryption

Use this command to enable encryption authentication for an OSPFv3 area. Use the **no** form of this command to restore the default settings.

area *area-id* **encryption ipsec spi** *spi* **esp [null |** [**des** | **3des | aes-cbc [128 | 192 | 256]**] [**0 | 7**] *des-key* **] [md5 | sha1**] [**0 | 7**] *key*

no area *area-id* **encryption**

Parameter Description

Parameter	Description
area-id	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Uses the null encryption mode.
des	Uses Data Encryption Standard (DES) encryption mode.
3des	Uses 3DES encryption mode.
aes-cbc[128 | 192 | 256]	Uses Advanced Encryption Standard-Cipher Block Chaining encryption mode. The key length is 128,192,256 bytes.
des-key	Encryption key
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
Key	Specifies an authentication key.

Defaults Encryption authentication is not performed by default.

Command Mode Routing process configuration mode

Usage Guide FSOS supports the null encryption mode and two authentication modes: MD5 and SHA1.

If encryption authentication is configured for an OSPFv3 area, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Encryption authentication configuration on interfaces, however, takes precedence over that of the OSPFv3 area.

Configuration Examples The following example specifies null encryption and MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
FS(config-router)# area 1 encryption ipsec spi 300 esp null md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description

ipv6 ospf encryption	Specifies interface encryption authentication.
area virtual-link encryption	Specifies virtual link encryption authentication.

Platform Description N/A

6.4 area-range

Use this command to set the range of the converged inter-area addresses. Use the **no** form of this command to restore the default settings.

area *area-id* **range** *ipv6-prefix/prefix-length* [**advertise | not-advertise**]

no area *area-id* **range** *ipv6-prefix/prefix-length*

Parameter Description

Parameter	Description
area-id	ID of the area in which the addresses are converged. It can be an integer or an IPv4 prefix.
ipv6-prefix/prefix-length	Range of the converged addresses.
advertise	Advertises the range of converged addresses.
not-advertise	The range of the converged addresses is not advertised. By default, the function is enabled.

Defaults No converged inter-area address range is defined by default.

Command Mode Routing process configuration mode

Usage Guide This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. The routing information combination only takes place on the area border. The specific routing information is seen on the intra-area routers, but only one converged route can be seen on the devices in other areas. By configuring the two options of advertise and not-advertise, you can decide whether to advertise the convergence range to enable blocking and filtering. By default, the range is advertised to the outside. The option cost can be used to set the metric value of convergence routing.

A number of route convergence commands can be defined. In this way, the number of the routes in the OSPF AS is reduced. Particularly for a large network, the forwarding performance will be improved.

When a number of routes are converged, and the containment relationship exists between items, the area range converged is determined by the longest match principle.

Configuration Examples The following example converges the routes in area 1.

```
ipv6 router ospf 1
area 1 range 2001:abcd:1:2::/64
```

Related

Command	Description

Commands

summary-prefix	Sets the range of the external routes to be converged.

Platform Description N/A

6.5 area stub

Use this command to create a stub area or set its attributes. Use the **no** form of this command to restore the default settings.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameter Description

Parameter	Description
area-id	ID of the stub area. It can be an integer or an IPv6 prefix.
no-summary	This option applies only to the ABR in the stub area, indicating that the ABR only advertises the type 3 LSA indicating the default route to the stub area, not other type 3 LSAs.

Defaults No stub area is defined by default.

Command Mode Routing process configuration mode

Usage Guide If an area is at the end of an entire network, it can be designed as the stub area, in which all the routers must execute the area stub command. If the area is designed as the stub area, it cannot learn the AS external routing information (type 5 LSAs). In practical application, the external routing information takes a large proportion of the link state database, so the devices in the stub area can only learn very little routing information, thus reducing the system resources required for the running of the OSPFv3 protocol.

By default, a type 3 LAS advertisement indicating default routing on the ABR in the stub area is generated, then the devices in the stub area can get to the outside of the AS.

If a totally stub area needs to be configured, just select the keyword **no-summary** when executing the **area stub** command on the ABR.

Configuration Examples The following example enables the ABR in stub area 10 to advertise the default route to the stub area.

```
ipv6 router ospf 1
area 10 stub
area 10 stub no-summary
```

Related Commands

Command	Description

area default-cost	Sets the cost of the default route in the stub area.

Platform Description N/A

6.6 area virtual-link

Use this command to create a virtual link or set its parameters. Use the **no** form of this command to restore the default settings.

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*] [**authentication ipsec spi** *spi* [**md5** | **sha1**] [**0** | **7**] *key*] [**encryption ipsec spi** *spi* **esp null** [**md5** | **sha1**] [**0** | **7**] *key*]

no area *area-id* **virtual-link** *router-id* [**hello-interval**] [**dead-interva**l] [**retransmit-interval**] [**transmit-delay**] [**instance**] [**authentication**] [**encryption**]

Parameter Description

Parameter	Description
area-id	ID of the area in which the virtual link is located. It can be an integer or an IPv6 prefix.
router-id	Neighbor router ID of the virtual link.
hello-interval *seconds*	Sets the interval to send the hello message on the local virtual link interface in the range from 1 to 65535 in the unit of seconds.
dead-interval *seconds*	Interval for the local interface of the virtual link to wait before considering that the neighbor fails. It is in the range from 1 to 65535 in the unit of seconds.
retransmit-interval *seconds*	Interval for retransmitting LSA on the local interface of the virtual link . The range is from 1 to 65535 in the unit of seconds.
transmit-delay *seconds*	Delay on the local interface of the virtual link in sending LSA. The range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	Specifies the instance corresponding to the virtual link. No virtual link can be established between different instances. Range: 0.-255
authentication ipsec spi *spi* [**md5** | **sha1**] [**0** | **7**] *key*	Specifies OSPFv3 authentication. ℹ Authentication configuration on two neighboring devices must be consistent. The **service password-encryption** command enables a key to be displayed in the cipher-text format. *spi* specifies a security parameter index, in the range from 256 to 4294967295. **md5** specifies the MD5 authentication mode. **sha1** specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. *key* specifies an authentication key.
encryption ipsec spi *spi* **esp null** [**md5**| **sha1**] [**0**|**7**] *key*	Specifies OSPFv3 encryption authentication. ℹ Authentication configuration on two neighboring devices must be

	consistent. The **service password-encryption** command enables a key to be displayed in the cipher-text format. *spi* specifies a security parameter index, in the range from 256 to 4294967295. **null** specifies the null encryption mode. **md5** specifies the MD5 authentication mode. **sha1** specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. *key* specifies an authentication key.
authentication ipsec spi *spi* [**md5 | sha1**] [**0 | 7**] *key*	Specifies OSPFv3 authentication. ⓘ Authentication configuration on two neighboring devices must be consistent. The **service password-encryption** command enables a key to be displayed in the cipher-text format. *spi* specifies a security parameter index, in the range from 256 to 4294967295. **md5** specifies the MD5 authentication mode. **sha1** specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. *key* specifies an authentication key.

Defaults

No virtual link is defined by default

hello-interval: 10 seconds; dead-interval: four times of the hello-interval; retransmit-interval: five seconds; transmit-interval: one second.

Authentication and encryption are not performed by default.

Command Mode

Routing process configuration mode

Usage Guide

In the OSPFv3 AS, all the areas must be connected with the backbone area to ensure that they can learn the routes of the whole OSPFv3 AS. If an area cannot be directly connected with the backbone area, it can connect it through a virtual link.

⚠ The virtual link shall not be in the stub or NSSA area.

⚠ **Hello-interval, dead-interval** and **instance** shall be configured consistently on both sides of the virtual link neighbors, otherwise neighboring relationship cannot be set up between the virtual neighbors.

Configuration Examples

The following example configures a virtual link.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# area 1 virtual-link 192.1.1.1
```

Related Commands

Command	Description
show ipv6 ospf	Displays the OSPFv3 routing process information.

show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.
show ipv6 ospf **virtual-links**	Displays the OSPFv3 virtual link information.

Platform Description

N/A

6.7 auto-cost

The metric of the OSPFv3 protocol is the interface-based bandwidth. Use this command to enable the bandwidth-based interface metric calculation or modify the reference bandwidth. Use the **no** form of this command to restore the default settings.

auto-cost [**reference-bandwidth** *ref-bw*]

no auto-cost [**reference-bandwidth**]

Parameter Description

Parameter	Description
reference-bandwidth *ref-bw*	Reference bandwidth in the range from 1 to 4294967 Mbps.

Defaults

The interface metric is calculated based on the reference bandwidth, which is 100Mbps.

Command Mode

Routing process configuration mode

Usage Guide

Use **no auto-cost reference-bandwidth** to restore it to the default reference bandwidth.

You can use **ipv6 ospf cost** in the interface configuration mode to set the cost of the specified interface, and it takes precedence over the metric calculated based on the reference bandwidth.

Configuration Examples

The following example changes the reference bandwidth to 10M.

```
ipv6 router ospf 1
auto-cost reference-bandwidth 5
```

Related Commands

Command	Description
ipv6 ospf cost	Sets the cost of an interface.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description

N/A

6.8 clear ipv6 ospf process

Use this command to clear and restart the OSPF process.

clear ipv6 ospf [*process-id*] **process**

Parameter Description

Parameter	Description
process-id	OSPF process ID, in the range from 1 to 65535

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

In normal case, it is not necessary to use this command.

Use the parameter *process-id* to clear only one specific OSPFv3 instance. If no *process-id* is specified, all the OSPFv3 instances will be cleared.

Configuration Examples

The following example restarts the OSPF process.

```
enble
clear ipv6 ospf process
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.9 default-information originate

Use this command to generate a default route to the OSPFv3 routing domain in the routing process mode. Use the **no** form of this command to restore the default settings.

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map*]

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map*]

Parameter Description

Parameter	Description
always	(Optional) It makes OSPFv3 generate the default route unconditionally, no matter whether the default route exists locally or not.
metric *metric*	(Optional) Initial metric value of the default route, in the range from 0 to 16777214
metric-type *type*	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different routers; type 2, the same metric seen on different routers.
route-map *map*	Associated route-map name, no associated route-map by default

Defaults

No default route is created;

The initial metric value is 1;

The default route type is type 2.

Command Mode

Routing process configuration mode

Usage Guide

When the **redistribute** or default-information command is executed, the OSPFv3-enabled router automatically turns into the autonomous system border router (ASBR). But the ASBR cannot generate the default route automatically or advertise it to all the routers in the OSPFv3 routing domain. The ASBR generates default routes by default. It is required to configure with the routing process configuration command **default-information originate**.

If the always parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route in the core routing table exists or not. However, the local router does not display the default route. To make sure whether the default route is generated, execute **show ipv6 ospf database** to observe the OSPF link state database. The execution of the **show ipv6 route** command on the OSPF neighbor will display the default route.

The metric of the external default route can be defined only with the **default-information originate** command and cannot be set with the **default-metric** command.

There are two types of OSPFv3 external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, type 1 takes precedence over type 2. As a result, the **show ipv6 route** command displays only the type 1 route.

This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area.

To generate a default route in the NSSA area, use the **area nssa default-information-originate** command.

The routers in the stub area cannot generate external default routes.

Configuration Examples

The following example generates a default route.

```
default-information originate always
```

Related Commands

Command	Description
redistribute	Redistribute routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf database	Displays the OSPFv3 link state database information.

Platform Description

N/A

6.10 default-metric

Use this command to set the default metric for the routes to be redistributed. Use the **no** form of this command to restore the default settings.

default-metric *metric-value*

no default-metric

Parameter Description

Parameter	Description
metric-value	Default metric for the routes to be redistributed. Its range is from 1 to 16777214.

Defaults The default is 20.

Command Mode The default route type is type 2.

Usage Guide This command can be used together with **redistribute** to set the default metric for the routes to be redistributed. But this command does not apply to two types of routes:

- The **default route generated** with default-information originate;
- The redistributed direct route, for which 20 is always the default metric value.

Configuration Examples The following example sets the default metric for the routes to be redistributed to 10.

```
default-metric 10
```

Related Commands

Command	Description
redistribute	Redistributes the routes.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description N/A

6.11 distance

Use this command to set the management distance corresponding to different types of OSPFv3 routes. Use the **no** form of this command to restore the default settings.

distance { *distance* | **ospf** { **intra-area** *distance* | **inter-area** *distance* | **external** *distance* } }

no distance [**ospf**]

Parameter Description

Parameter	Description
distance	Sets the management distance of the route, in the range from 1 to 255.
intra-area *distance*	Sets the management distance of the intra-area route, in the range from1 to 255.
inter-area *distance*	Sets the management distance of the inter-area route, in the range from 1 to 255.
external *distance*	Sets the management distance of the external route, in the range from 1 to 255.

Defaults The default value is 110.

Management distance of the intra-area route: 110,

Management distance of the inter-area route: 110

Management distance of the external-area route: 110.

Command Mode

Routing process configuration mode.

Usage Guide

This command is used to specify different management distances for different types of OSPFv3 routes. The management distance of the route is used for the comparison of routing priority, the smaller the management distance is, the higher the routing priority.

⚠ The priority of the route generated by different OSPFv3 processes must be compared using the management distance.

⚠ Setting the management distance as 255 indicates the routing entry is unreliable and will not for the packet forwarding.

Configuration Examples

The following example sets the OSPFv3 external route management distance to 160.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# distance ospf external 160
```

Related Commands

Command	Description
ipv6 router ospf	Enables the OSPFv3 routing process .

Platform Description

N/A

6.12 distribute-list in

Use this command to filter routes that are computed based on Link State Advertisement (LSA). Use the **no** form of this command to restore the default settings.

distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

Parameter Description

Parameter	Description
name	Specifies an ACL filtering rule.
prefix-list *prefix-list-name*	Specifies a prefix list filtering rule.
interface-type interface-number	Specifies an interface on which LSA-based routes are filtered.

Defaults

Routes are not filtered by default.

Command Mode

Routing process configuration mode

Usage Guide Filter the routes computed based on LSA. Only the routes meeting filtering conditions can be forwarded. Route filtering does not affect the link state database and the routing tables of the neighbors. The ACL and prefix list filtering rules cannot be set at the same time. You can set only the ACL filtering rule or the prefix list filtering rule for a specific interface.

The routing filtering rules affect only forwarding of local routes but not route computation based on LSA. When route filtering is configured on an ABR, LSA can still compute routes and generate and send inter-area LSAs with prefixes to other areas. This will cause blackhole routes. To prevent the generation of blackhole routes, you can run the **area range** command with the **not-advertise** keyword.

Configuration Examples The following example filters routes that are computed based on Link State Advertisement (LSA).

```
FS(config)# ipv6 prefix-list aaa seq 10 permit 2001::/64
FS(config)# ipv6 router ospf 25
FS(config-router)# redistribute rip metric 100
FS(config-router)# distribute-list prefix-list aaa in ethernet 0/1
```

Related Commands

Command	Description
area range	Configures route aggregation in an area.

Platform Description N/A

6.13 distribute-list out

Use this command to filter routes that are re-distributed. This command has the similar function as the **redistribute** command. Use the **no** form of this command to restore the default settings.

distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

Parameter Description

Parameter	Description
name	Specifies the ACL filtering rule.
prefix-list *prefix-list-name*	Specifies the prefix list filtering rule.
bgp | connected | isis [*area-tag*] | **ospf** process-id | **rip** | **static**	Specifies the source from which the routes are filtered.

Defaults Routes are not filtered by default.

Command Mode Routing process configuration mode

Usage Guide

The **distribute-list out** command has the similar function as the **redistribute route-map** command. It can be used to filter the routes that are re-distributed based on other protocols into an OSPFv3 area. It does not directly re-distribute routes but works with the **redistribute** command to re-distribute routes. The ACL and prefix list filtering rules cannot be configured at the same time. You can set only the ACL filtering rule or the prefix list filtering rule to filter the routes from a specific source.

Configuration Examples

The following example filters static routes that are re-distributed.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# redistribute static
FS(config-router)# distribute-list prefix-list jjj out static
```

Related Commands

Command	Description
redistribute	Re-distributes routes that are carried by other routing processes.

Platform Description

N/A

6.14 enable mib-binding

Use this command to bind MIB to a specific OSPFv3 process. Use the **no** form of this command to restore the default settings.

enable mib-binding

no enable mib-binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults

MIB is bound to an OSPFv3 process with the smallest process number by default.

Command Mode

Routing process configuration mode

Usage Guide

OSFPv3 MIB has no configuration information about OSFPv3 processes. You can operate only one OSFPv3 process through SNMP. OSFPv3 MIB is bound to the OSFPv3 process with the smallest process number by default. Users' operations take effect on this process.

To operate a specific OSFPv3 process through SNMP, you can bind OSFPv3 MIB to the process.

Configuration Examples

The following example enables users to operate the OSPFv3 process with the process number of 100 through SNMP.

```
FS(config)# ipv6 router ospf 100
FS(config-router)# enable mib-binding
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.
enable traps	Enables the OSPFv3 trap function.

Platform Description

N/A

6.15 enable traps

OSPFv3 processes support eight types of trap information, which are classified into two categories. Use this command to send specific trap information. Use the **no** form of this command to restore the default settings.

enable traps [**error** [**IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket**] | **state-change** [**IfStateChange | NbrStateChange | NssaTranslatorStatusChange | VirtIfStateChange | VirtNbrStateChange**]]

no enable traps [**error** [**IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket**] | **state-change** [**IfStateChange | NbrStateChange | NssaTranslatorStatusChange | VirtIfStateChange | VirtNbrStateChange**]]

Parameter Description

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><b>Error</b></td><td>Configures all error-related trap types. This keyword can also specify the following types of error traps:
<table>
<tr><td><b>IfConfigError</b></td><td>Specifies an interface parameter error;</td></tr>
<tr><td><b>IfRxBadPacket</b></td><td>Specifies incorrect packets received by an interface;</td></tr>
<tr><td><b>VirtIfConfigError</b></td><td>Specifies a parameter error on a virtual interface;</td></tr>
<tr><td><b>VirtIfRxBadPacket</b></td><td>Specifies incorrect packets received by a virtual interface.</td></tr>
</table></td></tr>
<tr><td><b>state-change</b></td><td>Configures all traps related to state change. This keyword can also specify the following traps related to state change:
<table>
<tr><td><b>IfStateChange</b></td><td>Specifies state change of an interface;</td></tr>
<tr><td><b>NbrStateChange</b></td><td>Specifies state change of a neighbor;</td></tr>
<tr><td><b>NssaTranslatorStatusChange</b></td><td>Specifies status change of the NSSA translator.</td></tr>
<tr><td><b>VirtIfStateChange</b></td><td>Specifies state change of a virtual interface;</td></tr>
<tr><td><b>VirtNbrStateChange</b></td><td>Specifies state change of a virtual neighbor.</td></tr>
</table></td></tr>
</table>

Defaults

All traps are disabled by default.

Command Mode

Routing process configuration mode

Usage Guide

Before configuring this command, you must run the **snmp-server enable traps ospf** command; otherwise, OSPFv3 trap information cannot be sent correctly**.** This is because the function of this command is restricted by the **snmp-server** command.

You can synchronously enable the trap function of different processes even if MIB is not bound to these processes.

Configuration Examples

The following example enables all traps of OSPFv3 process 100.

```
FS(config)#ipv6 router ospf 100
FS(config-router)# enable traps
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.
enable mib-binding	Binds MIB to an OSPFv3 process.
snmp-server enable traps ospf	Enables OSPFv3 to send trap information.

Platform Description

N/A

6.16 graceful-restart

Use this command to enable the OSPFv3 graceful restart (GR) function and to set the GR period. Use the **no** form of this command to restore the default settings.

graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

no graceful-restart [*graceful-period*]

Parameter Description

Parameter	Description
grace-period *grace-period*	Configures the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment when OSPFv3 gracefully restarts. The GR period is in the range from 1 to 1800 in the unit of seconds. The default is 120.
inconsistent-lsa-checking	Configures the topology change detection. Once the topology change is detected, the device will exit GR and finish the convergence, This function is enabled by default after GR is enabled.

Defaults

This function is enabled by default.

Command Mode

Routing process configuration mode

Usage Guide

GR is configured based on the OSPFv3 instance. Different instances could be configured with different parameters.

Use this command to configure the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment that OSPFv3 gracefully restarts. In this period, the device will perform link reconstruction to restore OSPFv3. When the GR period expires, OSPFv3 exits GR and finishes regular operation.

To enable the GR function and set the GR period to the 120 seconds, use the **graceful-restart** command. To modify the GR period, use the **graceful-restart grace-period** command. Topology stability is indispensable for uninterrupted forwarding. If topology changes, OSPFv3 finishes convergence instead of continuing GR to avoid long time interruption

1) Disabling the topology change detection: If the topology cannot converge in time in the hot backup process, the long term forwarding interruption may occur.

2) Enabling the topology change detection: Forwarding interruption may occur but the interruption time is much shorter than the time it takes to disable topology detection.

It is not recommended to disable the topology change detection. In some scenario where long term forwarding interruption does not occur, disabling the topology change detection minimizes the forwarding interruption time.

The GR function is unavailable when the Fast Hello function is enabled.

Configuration Examples

The following example enables GR for OSPFv3 instance 1 and sets the GR period to 60 seconds.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# graceful-restart
FS(config-router)# graceful-restart grace-period 60
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.17 graceful-restart helper

Use this command to enable the OSPFv3 graceful restart helper function. Use the **no** form of this command to disable this function.

graceful-restart helper disable

no graceful-restart helper disable

Use this command configure the topology change detection method of OSPFv3 GR helper. Use the **no** form of this command to cancel the configuration.

graceful-restart helper { **strict-lsa-checking** | **internal-lsa-checking**}

no graceful-restart helper {**strict-lsa-checking** | **internal-lsa-checking**}

Parameter Description

Parameter	Description
disable	Disables the device to assist other devices in performing GR.
strict-lsa-checking	Checks the change of the LSA of types 1-5 and 7 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.
internal-lsa-checking	Checks the change of the LSA of types 1–3 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.

Defaults

The GR helper is enabled by default.

The device where the GR helper is enabled does not check the LSA change by default.

Command Mode

Routing process configuration mode

Usage Guide

Use this command to enable the GR helper function. When one neighbor device performs graceful restart, the Grace-LSA is advertised to all neighbors. If the device enabled with the GR helper receives the Grace-LSA, it will become the GR Helper to help the neighbors perform GR. The **disable** option means that it is not allowed to perform the GR helper function for any device in GR.

The GR helper does not perform the network change detection by default. The convergence is not performed again until the GR is implemented even if the network changes. Use the **strict-lsa-checking orinternal-lsa-checking** command to enable the device to detect the change of network topology during the GR. The former checks any LSA (types 1-5,7) that stands for the network information, the latter checks the LSA that stands for the AS inner-area route. In the large scale network, it is not recommended to enable the LSA check option because the partial network changes trigger the ending of the GR, decreasing the convergence speed of the entire network.

Configuration Examples

The following example disables the GF helper function of the OSPFv3 instance 1 and modifies the topology change detection policy.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# graceful-restart helper disable
FS(config-router)# no graceful-restart helper disable
FS(config-router)# graceful-restart helper strict-lsa-checking
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.18 ipv6 ospf area

Use this command to enable the interface to participate in the OSPFv3 routing process. Use the **no** form of this command to restore the default settings.

ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

Parameter Description

Parameter	Description
process-id	OSPF process ID.
area *area-id*	OSPFv3 area in which the interface participates. It can be an integer or an IPv4 prefix.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface. Range: 0-255.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode.

Usage Guide

Run this command to enable the OSPFv3 on an interface, and then configure the OSPFv3 process with **ipv6 router osp**. The interface will be automatically started after this command is used.

Use **no ipv6 ospf area** to disable the specified interface to participate in the OSPFv3 routing process.

Use **no ipv6 router ospf** to disable all the interfaces to participate in the OSPFv3 routing process.

The neighbor relationship can only be established between the routers with the same instance ID.

After this command is configured, all the prefix information on the interface will be used in the operation of the OSPFv3.

Configuration Examples

The following example starts the OSPFv3 process on int fastethernet 0/0 for the specified area of the specified instance.

```
int fastethernet 0/0
ipv6 ospf 1 area 2 instance 2
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
passive-interface	Setsthe a passive interface.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description

N/A

6.19 ipv6 ospf authentication

Use this command to configure OSPFv3 interface authentication. Use the **no** form of this command to restore the default settings.

ipv6 ospf authentication [**null | ipsec spi** *spi* [**md5** [**string-key**] **| sha1**] [**0 | 7**] *key*] [**instance** *instance-id*]

no ipv6 ospf authentication

Parameter Description

Parameter	Description
null	Indicates that authentication is not performed.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
md5	Specifies the MD5 authentication mode.
string-key	Indicates that MD5 authentication key supports special characters.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
key	Specifies an authentication key.
instance *instance-id*	Configure the OSPFv3 instance specified on the interface. Range: 0-225.

Defaults

Authentication is not performed by default.

Command Mode

Interface configuration mode

Usage Guide

FSOS supports three authentication modes:

- null authentication mode, which is configured when authentication is not needed
- MD5 authentication mode
- SHA1 authentication mode

ⓘ OSPFv3 authentication parameters configured on interconnected interfaces must be consistent.

Configuration Examples

The following example specifies MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
FS(config-if)# ipv6 ospf authentication ipsec spi 300 md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
ipv6 ospf authentication	Specifies interface authentication.
area virtual-link authentication	Specifies virtual link authentication.

Platform Description

N/A

6.20 ipv6 ospf cost

Use this command to set the cost of the interface. Use the **no** form of this command to restore the default settings.

ipv6 ospf cost *cost* [**instance** *instance-id*]

no ipv6 ospf cost [**instance** *instance-id*]

Parameter Description

Parameter	Description
cost	Cost of interface, in the range from 0 to 65535.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

The default interface cost is the reference bandwidth/Bandwidth (100Mbps by default).

Command Mode

Interface configuration mode.

Usage Guide

By default, the cost of the OSPFv3 interface is 100Mbps/Bandwidth, in which the Bandwidth is the bandwidth of the interface and configured with the command **bandwidth** in the interface configuration mode.

The default costs of OSPFv3 interfaces for several typical lines are:

- 64K serial line: 1562;
- E1 line: 48
- 10M Ethernet: 10
- 100M Ethernet: 1

The OSPFv3 cost configured with the command **ipv6 ospf cost** will overwrite the default configuration.

Configuration Examples

The following example sets the cost of the interface to 1:

```
FS(config)# int fastethernet 0/0
FS(config-if)# ipv6 ospf cost 1
```

Related Commands

Command	Description
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description

N/A

6.21 ipv6 ospf dead-interval

Use this command to set a dead interval of neighbors on an interface. If no hello packet is received from a neighbor within the interval, the neighboring relationship is considered to fail. Use the **no** form of this command to restore the default settings.

ipv6 ospf dead-interval { *seconds* | **minimal hello-multiplier** *multiplier* } [**instance** *instance-id*]

no ipv6 ospf dead-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	Dead interval of neighbors. Its range is from 1 to 65535 in the unit of seconds.
minimal hello-multiplier *multiplier*	Enables the fast hello function, which takes 1s as the dead interval of neighbors. *Multiplier* specifies the number of hello packets sent in one second, in the range from 3 to 20.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

If the fast hello function is not enabled, the dead interval of neighbors is four times longer than the hello interval.

⚠ If the hello interval is changed, the dead interval of neighbors varies automatically.

Command Mode

Interface configuration mode

Usage Guide

The dead interval of neighbors must be longer than the hello interval.

The OSPFv3 fast hello function allows OSPFv3 to fast discovery neighbors and detect whether neighboring relationships are valid. To enable the OSPFv3 fast hello function, you can specify the **minimal** and **hello-multiplier** keywords and the *multiplier* parameter in this command. **minimal** specifies the deal interval of neighbors to be 1s; **hello-multiplier** specifies the number of times that hello packets are sent in a second. Therefore, this configuration reduces the hello interval to be shorter than 1s.

If an interface is enabled with the fast hello function, the **hello-interval** field of hello packets to be advertised by this interface is set to 0, and that of hello packets received from this interface is omitted**.**

ℹ **dead-interval**, **minimal**, and **hello-multiplier** that are introduced to enable the fast hello function cannot be configured together with **hello-interval**.

No matter whether the fast hello function is configured, the dead interval of neighbors on the interconnected interfaces of neighbors must be consistent. The values of **hello-multiplier** on the interconnected interfaces can be different but you must ensure that at least one hello packet is received within the dead interval of neighbors.

You can use the **show ipv6 ospf interface** command to monitor the dead interval of neighbors and the fast hello interval on an interface.

Configuration Examples

The following example sets the dead interval of neighbors to 60 seconds on an interface.

```
FS(config)# int fastethernet 0/0
FS(config-if)# ipv6 ospf dead-interval 60
```

Related

Command	Description

Commands

ipv6 ospf hello-interval	Sets the interval for sending the Hello message on an interface.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process

Platform Description

N/A

6.22 ipv6 ospf encryption

Use this command to enable OSPFv3 encryption authentication on an interface. Use the **no** form of this command to restore the default settings.

ipv6 ospf encryption [**null | ipsec spi** *spi* **esp [null |** [**des** | **3des | aes-cbc [128 | 192 | 256]**] [**0 | 7**] *des-key* **]** [**md5 | sha1**] [**0 | 7**] *key*] [**instance** *instance-id*]

no ipv6 ospf encryption [**instance** *instance-id*]

Parameter Description

Parameter	**Description**
null	Indicates that encryption authentication is not performed.
spi	Specifies a security parameter index, in the range from 256 to 4294967295.
null	Specifies the null encryption mode.
des	Uses Data Encryption Standard (DES) encryption mode.
3des	Uses 3DES encryption mode.
aes-cbc[128 | 192 | 256]	Uses Advanced Encryption Standard-Cipher Block Chaining encryption mode. The key length is 128,192,256 bytes.
des-key	Encryption key
md5	Specifies the MD5 authentication mode.
sha1	Specifies the SHA1 authentication mode.
0	Indicates that a key is displayed in the plain-text format.
7	Indicates that a key is displayed in the cipher-text format.
key	Specifies an authentication key.

Defaults

Encryption authentication is not performed by default.

Command Mode

Interface configuration mode

Usage Guide

FSOS supports the 3 encryption modes: DES, 3DES and AES-CBC, and 2 authentication modes: MD5 and SHA1

OSPFv3 encryption authentication parameters configured on interconnected interfaces must be consistent.

Configuration

The following example specifies null encryption and MD5 authentication in OSPFv3 interface configuration mode

Examples and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

```
FS(config-if)# ipv6 ospf encryption ipsec spi 300 esp null md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Related Commands

Command	Description
area encryption	Specifies area encryption authentication.
area virtual-link encryption	Specifies virtual link encryption authentication.

Platform Description N/A

6.23 ipv6 ospf hello-interval

Use this command to set the interval for the interface to send the Hello message. Use the **no** form of this command to restore the default settings.

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf hello-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	Interval for sending the Hello message. Its range is from 1 to 65535 in the unit of seconds.
instance i*nstance-id*	Configures the specific OSPFv3 instance on the interface.

Defaults The broadcast network and point-to-point network :10 seconds. The point-to-multipoint network and NBMA network :30 seconds.

Command Mode Interface configuration mode.

Usage Guide The same hello sending intervals must be set for the neighbors, otherwise the normal adjacency cannot be established.

The dead-interval minimal hello-multiplier and hello-interval parameters for Fast Hello cannot be configured simultaneously.

Configuration Examples The following example sets the interval for the interface to send the Hello message to 20 seconds.

```
ipv6 ospf hello-interval 20
```

Related Commands

Command	Description
ipv6 ospf dead-interval	Sets the interval for the interface to consider that the neighbor fails.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description

N/A

6.24 ipv6 ospf mtu-ignore

Use this command to ignore the MTU check when an interface receives the database description message. Use the **no** form of this command to restore the default settings.

ipv6 ospf mtu-ignore [**instance** *instance-id*]

no ipv6 ospf mtu-ignore [**instance** *instance-id*]

Parameter Description

Parameter	Description
instance *instance-id*	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

The MTU check is enabled by default.

Command Mode

Interface configuration mode.

Usage Guide

After receiving the database description message, the OSPFv3 device will check whether the MTU of neighbor interface is the same as its own MTU. If the received database description message indicates an MTU greater than its own interface's MTU, the neighbor relationship cannot be established. This can be fixed by disabling the MTU check.

Configuration Examples

The following example disables the MTU check function on the ethernet 1/0.

```
FS(config)# interface ethernet 1/0
FS(config-if)# ipv6 ospf mtu-ignore
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 mtu	Sets the value of IPv6 MTU of the interface.

Platform Description

N/A

6.25 ipv6 ospf neighbor

Use this command to configure the OSPFv3 neighbor manually. Use the **no** form of this command to restore the default settings.

ipv6 ospf neighbor *ipv6-address* [[**cost** <1-65535>] [poll-interval <0-2147483647> | priority <0-255>]] [instance

instance-id]

no ipv6 ospf neighbor *ipv6-address* [[cost <1-65535>] [**poll-interval** < 0-2147483647 > | **priority** < 0-255 >]] [**instance** *instance-id*]

Parameter Description

Parameter	Description
cost *cost*	(Optional) Configures the cost to each neighbor in point-to-multipoint network. It is not defined by default, where the cost configured on the interface will be used. It ranges from 1 to 65535. Only the networks of the point-to-multipoint type support this option.
poll-interval *seconds*	(Optional) Interval for polling the neighbors (in seconds), which ranges from 1 to 2147483647. Only the networks of the non-broadcast (NBMA) type support this option.
priority *priority*	(Optional) Configures the priority value of non-broadcast network neighbors, which ranges from 0 to 255. Only the non-broadcast (NBMA) type network supports this option.
instance *instance-id*	(Optional) Configures the specific OSPFv3 instance on the interface, which ranges from 0 to 255.

Defaults

No neighbor is defined;

Neighbor polling interval: 120 seconds;

Priority value of non-broadcast network neighbor: 0.

Command Mode

Interface configuration mode.

Usage Guide

You can set relevant parameters for the neighbors depending on the actual network type.

Configuration Examples

The following example shows how to configure the OSPFv3 neighbor as follows: IPv6 address: 2001:DB8:4::1, priority value: 1, polling interval: 150 seconds.

```
FS(config)# interface fastEthernet 0/1
FS(config-if)# ipv6 ospf neighbor 2001:DB8:4::1 priority 1 poll-interval 150
```

Related Commands

Command	Description
Ipv6 ospf priority	Sets the priority value of an interface.
Ipv6 ospf network	Sets the network type of an interface.

Platform Description

N/A

6.26 ipv6 ospf network

Use this command to set the network type of the interface. Use the **no** form of this command to restore the default settings.

ipv6 ospf network { **broadcast** | **non-broadcast** | **point-to-point** | **point-to-multipoint** [**non-broadcast**] } [**instance** *instance-id*]

no ipv6 ospf network [**broadcast** | **non-broadcast** | **point-to-point** | **point-to-multipoint** [**non-broadcast**]] [**instance** *instance-id*]

Parameter Description

Parameter	Description
broadcast	Specifies the broadcast network type.
non-broadcast	Specifies the non-broadcast network type.
point-to-point	Specifies the point-to-point network type.
point-to-multipoint	Specifies the point-to-multipoint network type.
point-to-multipoint non-broadcast	Specifies the point-to-multipoint non-broadcast network type.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface with the valid id range from 0 to 255.

Defaults

Point-to-point network type: PPP, SLIP, frame relay point-to-point sub-interface and X.25 point-to-point sub-interface encapsulation.

NBMA network type: frame relay(except for the point-to-point sub-interface) and X.25 encapsulation (except for the point-to-point sub-interface)

Broadcast network type: Ethernet encapsulation.

The point-to-multipoint network type is not the default type.

Command Mode

Interface configuration mode.

Usage Guide

You can set the network type of the interface according to the actual link type applied and the topology.

Configuration Examples

The following example sets the network type of the interface that participates in the OSPFv3 to point-to-point.

```
FS(config)# interface ethernet 1/0
FS(config-if)# ipv6 ospf network point-to-point
```

Related Commands

Command	Description
ipv6 ospf priority	Sets the interface priority.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description

N/A

6.27 ipv6 ospf priority

Use this command to set the interface priority. Use the **no** form of this command to restore the default settings.

ipv6 ospf priority *number-value* [**instance** *instance-id*]

no ipv6 ospf priority [**instance** *instance-id*]

Parameter Description

Parameter	Description
number-value	The priority of the interface. Its range is from 0 to 255.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface. Its range is from 0 to 255.

Defaults

The default priority is 1.

Command Mode

Interface configuration mode.

Usage Guide

In the broadcast network type, it is necessary to elect the DR/BDR. In electing the DR/BDR, the device of a higher priority is preferred. If several devices are of the same priority, the one with the largest router-ID is preferred.

The device with the priority level of 0 does not participate in the election of DR/BDR.

Configuration Examples

The following example disables the interface from being elected as the DR/BDR.

```
FS(config)# interface ethernet 1/0
FS(config-if)# ipv6 ospf priority 0
```

Related Commands

Command	Description
ipv6 ospf network	Sets the network type of an interface.
router-id	Sets the ID of a router.
show ipv6 ospf interface	Displays the OSPFv3 interface information.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface.

Platform Description

N/A

6.28 ipv6 ospf retransmit-interval

Use this command to set the interval for the interface to retransmit the LSA. Use the **no** form of this command to restore the default settings.

ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

no ipv6 ospf retransmit-interval [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	Interval for retransmitting the LSA. Its range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	Configures the specific OSPFv3 instance on the interface.

Defaults

The default is five seconds.

Command Mode

Interface configuration mode.

Usage Guide

To ensure the reliability of the routing information transmission, the LSA sent to the neighbor shall be acknowledged by the neighbor. You can use this command to set the interval for the acknowledgement by the neighbor. If no acknowledgement is received within the specified period, the LSA information will be retransmitted.

Configuration Examples

The following example sets the interval for retransmitting the LSA to 10 seconds.

```
FS(config)# interface ethernet 1/0
FS(config-if)# ipv6 ospf retransmit-interval 10
```

Related Commands

Command	Description
show ipv6 ospf interface	Displays the OSPFv3 interface information.
ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.

Platform Description

N/A

6.29 ipv6 ospf transmit-delay

Use this command to set the delay on the interface in sending the LSA. Use the **no** form of this command to restore the default settings.

ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]

no ipv6 ospf transmit-delay [**instance** *instance-id*]

Parameter Description

Parameter	Description
seconds	The delay in sending LSA. Its range is from 1 to 65535 in the unit of seconds.
instance *instance-id*	Configures the ID of a specific OSPFv3 instance on the interface, in the range from 0 to 255.

Defaults

The default is one second.

Command Mode

Interface configuration mode.

Usage Guide

Use this command to set the delay on the interface in transmitting the LSA.

Configuration Examples

The following example sets the delay on the interface in transmitting the LSA.

```
FS(config)# interface ethernet 1/0
FS(config-if)# ipv6 ospf transmit-delay 2
```

Related Commands

Command	Description
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description

N/A

6.30 ipv6 router ospf

Use this command to start the OSPFv3 routing process. Use the **no** form of this command to restore the default settings.

ipv6 router ospf *process-id* [**vrf** *vrf-name*]

no ipv6 router ospf *process-id*

Parameter Description

Parameter	Description
process-id	OSPFv3 process ID number. Without the process number configured, it indicates that process 1 is started.
vrf-name	Specifies the VRF that OSPFv3 process belongs to.

Defaults

No OSPFv3 routing process is started.

Command Mode

Global configuration mode.

Usage Guide

After the OSPFv3 process is started, the routing process configuration mode is entered.

At present, our products support up to 32 OSPFv3 processes.

Configuration Examples

The following example starts OSPFv3 process in the specified VRF VPN1.

```
FS(config)# ipv6 router ospf 1 vrf vpn_1
```

Related Commands

Command	Description
ipv6 ospf area	Configures an interface to participate in the OSPFv3

	routing process.
show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description N/A

6.31 ipv6 router ospf max-concurrent-dd

Use this command to set the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes. Use the **no** form of this command to restore the default settings.

ipv6 router ospf max-concurrent-dd *number*

no ipv6 router ospf max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum concurrent interacting neighbors, in the range from 1 to 65535.

Defaults The default is 5.

Command Mode Global configuration mode

Usage Guide When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes can be restricted.

Configuration Examples The following example sets the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.

```
FS#conf terminal
FS(config)#ipv6 router ospf max-concurrent-dd 4
```

Related Commands

Command	Description
max-concurrent-dd	Sets the maximum concurrent interacting neighbors in the OSPFv3 processes

Platform Description N/A

6.32 log-adj-changes

Use this command to enable the logging of adjacency changes. Use the **no** form of this command to restore the default settings.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Parameter Description

Parameter	Description
detail	Displays details of adjacency changes

Defaults By default, the adjacency state log on the entry of or exit from the FULL state is output.

Command Mode Routing process configuration mode

Usage Guide N/A

Configuration Examples The following example turns on the log of adjacency state change.

```
FS(config)# router ospf 1
FS(config)# log-adj-changes detail
```

Related Commands

Command	Description
show ipv6 ospf	Displays the OSPF global configuration information

Platform Description N/A

6.33 max-concurrent-dd

Use this command to set the maximum number of DD packets that can be processed concurrently in the OSPFv3 routing process. Use the **no** form of this command to restore the default settings.

max-concurrent-dd *number*

no max-concurrent-dd

Parameter Description

Parameter	Description
number	Maximum number of DD packets that can be processed concurrently, in the range from 1 to 65535.

Defaults The default is 5.

Command Mode Routing process configuration mode.

Usage Guide When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in each OSPFv3 instance can be restricted.

Configuration Examples

The following example sets the maximum concurrent interacting neighbors allowed in the current OSPFv3 routing process to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.

```
router ipv6 ospf 1
max-concurrent-dd 4
```

Related Commands

Command	Description
ipv6 router ospf max-concurrent-dd	Sets the maximum concurrent interacting neighbors allowed in the OSPFv3 processes.

Platform Description

N/A

6.34 passive-interface

Use this command to set the passive interface. Use the **no** form of this command to restore the default settings.

passive-interface { **default** | *interface-type interface-number* }

no passive-interface { **default** | *interface-type interface-number* }

Parameter Description

Parameter	Description
default	Sets all the interfaces to passive ones.
interface-type interface-number	Sets the specified interface to a passive one.

Defaults

No passive interface is set by default.

Command Mode

Routing process configuration mode

Usage Guide

After an interface is set to a passive one, it no longer receives or sends the hello message.

This command applies to the interfaces participating in the OSPFv3 but not to the virtual links.

Configuration Examples

The following example enables only the VLAN1 interface to participate in the OSPFv3 process.

```
passive-interface default
no passive-interface vlan 1
```

Related Commands

Command	Description
ipv6 ospf area	Configures an interface to participate in the OSPFv3

	routing process.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.

Platform Description N/A

6.35 redistribute

Use this command to start the route redistribution in order to import the routing information of other routing protocols to the OSPFv3 routing process. Use the **no** form of this command to restore the default settings.

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*]

no 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-type** { *1*|*2* } | **route-map** *route-map-name* | tag *tag-value*]

Parameter Description

Parameter	**Description**
bgp	The bgp protocol is redistributed.
connected	The directly connected route is redistributed.
isis*[area-tag]*	The isis is redistributed. The area-tag specifies a particular isis instance.
ospf *process-id*	The ospf is redistributed. The process-id specifies a particular ospf instance within the range of 1-65535.
rip	The rip is redistributed.
static	The static route is redistributed.
level-1| **level-1-2**| **level-2**	It is used in the IS-IS route redistribution only and redistributes the routes at a specified level. .
match	It is used in the OSPFv3 route redistribution only and filters specific routes for redistribution; internal: inter-area and intra-area routes. external [1|2]: E1, E2 or all external routes. Nssa-external [1 | 2]: N1, N2 or all external routes of the NSSA area. All sub-type OSPFv3 routes are redistributed by default.
metric *metric-value*	Specifies the metric for the OSPFv3 external 2 LSA with metric-value. Its range is 0 to 16777214.
metric-type *{ 1|2 }*	Set the metric type for the external route to E-1 or E-2.
route-map *route-map-name*	Specifies the routing policy for route redistribution. The name of map-tag can be composed of up to 32 characters. No route-map is associated by default.
tag *tag-value*	Specifies the tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.

Defaults

The function is disabled by default;

Metric-type: 2;

Level-2 routes are redistributed in the ISIS redistribution

OSPFv3 routes of all sub-types are redistributed in the OSPFv3 redistribution

No route-map is associated

Command Mode

Routing process configuration mode

Usage Guide

When a device supports multiple routing protocols, the coordination between these protocols becomes an important task. The device can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols.

The parameters level-1, level-2 or level-1-2 can be configured in the redistribution of the ISIS routes to indicate the level of the routes in the redistribution. By default, the level-2 ISIS routes are redistributed

When redistributing OSPFv3 routes, you can configure *match* to redistribute the routes of the corresponding sub-type among the redistributed OSPFv3 routes. All types of OSPFv3 routes are redistributed by default.

The *match* parameter of route-map is specific to the source of routes. The parameters *tag*, *metric* and *metric-type* of the set rule of route-map take precedence over the ones configured for the redistribute command.

⚠ The metric value of the route-map associated should be in the range of 0 to 16777214. If the metric value is not in this range, the route cannot be introduced.

The rules for the **no** form of the **redistribute** command are as follows:

If some parameters are specified in the no command, restore their default settings;

If no parameters are specified in the **no** command, delete the whole command.

For example, if the configuration is made below:

Now modify the configuration with the command no redistribute isis 112 level-2

According to the above rules, the command only restores level-2 to default and level-2 is default per se, so after the above no command is executed, the configuration remains as

redistribute isis 112 level-2

To delete the whole command, use the command below

Configuration Examples

The following example redistributes the direct route and associates route-map test:

```
ipv6 router ospf 1
redistribute connect metric 10 route-map test
```

The associated route-map is configured as follows:

```
route-map test permit 10
match metric 20
set metric 30
```

The effect of the above configuration is to set the metric value which is 20 of the redistributed routes to 30, and that of other routes to 10

Related Commands

Command	Description

default-information originate	Sets the default route to be redistributed.
default-metric	Sets the default metric for the route to be redistributed.
summary-prefix	Sets the converged address range of the external route.
show ipv6 ospf	Displays the OSPFv3 routing process information.
show ipv6 ospf database	Displays the OSPFv3 link state database information.

Platform Description

N/A

6.36 router-id

Use this command to set the router ID (device ID). Use the **no** form of this command to restore the default settings.

router-id *router-id*

no router-id

Parameter Description

Parameter	Description
router-id	ID of the device in the IPv4 address format.

Defaults

The OSPFv3 routing process, the largest IPv4 address of all loopback interfaces is elected as the router ID; If there is no loopback interface with an IPv4 address, the OSPFv3 process will elect the largest IPv4 of all other interfaces as the router ID

Command Mode

Routing process configuration mode

Usage Guide

Each device that runs the OSPFv3 process shall be identified with a router ID. Router ID is in the format of IPv4 address.

Any IPv4 address can be set as the router ID, but the router ID of every routers in the AS must be unique. If multiple OSPFv3 processes are running on the same device, the router ID of every process must be unique. Note that the change of the router ID results in considerable processing work in the protocol. Therefore, it is not recommended to change any router ID without proper reason. A prompt will be given to ask whether you are sure to modify the router ID. It is recommended that you specify a router ID once an OSPFv3 process starts before configuring other parameters for the process

Configuration Examples

The following example sets the ID of the device that participates in the OSPFv3 process to 1.1.1.1.

```
router-id 1.1.1.1
```

Related Commands

Command	Description
ipv6 ospf priority	Sets the interface priority.

show ipv6 ospf	Displays the OSPFv3 routing process information.

Platform Description N/A

6.37 summary-prefix

Use this command to configure the converged route outside the OSPFv3 routing domain in the routing process configuration mode. Use the **no** form of this command to restore the default settings.

summary-prefix *ipv6-prefix/prefix-length* [**not-advertise** | [**tag** *number*] [**cost** *cost*]]

no summary-prefix *ipv6-prefix/prefix-length* [**not-advertise |** [**tag**] [**cost**]]

Parameter Description

Parameter	Description
ipv6-prefix/prefix-length	Address range of the converged route
not-advertise	Does not advertise the converged route to neighbors. Absence of this parameter means to advertise.
tag *number*	Tag value redistributed to the OSPFv3 inner route, in the range from 0 to 4294967295.
cost *cost*	Cost value of converged route, in the range from 0 to 16777214.

Defaults No converged route is configured by default.

Command Mode Routing process configuration mode.

Usage Guide When routes are redistributed by another routing process into the OSPFv3 routing process, every route is advertised to the OSPFv3-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous system border device can advertise only one converged route, thus reducing the scale of routing table greatly.

It is different from the **area range** command. The area range involves the convergence of routes between OSPFv3 areas, while the **summary-prefix** involves the convergence of external routes of the OSPFv3 routing domain.

Configuring the **summary-prefix** command on the ASBR can perform convergence for only redistributed routes; while configuring this command on the NSSA ABR translator can perform convergence for the redistributed routes and the Type-5 routes translated from Type-7.

Configuration Examples The following example configures the external route within the 2001:DB8::/64 to the converged route 2001:DB8::/64 to advertise it.

```
summary-prefix 2001 :DB8 : : /64
```

Related Commands

Command	Description
area-range	Configures route convergence between the OSPFv3

	areas.
redistribute	Redistributes the routes in other routing process.

Platform Description N/A

6.38 show ipv6 ospf

Use this command to display the information of the OSPFv3 process.

show ipv6 ospf [*process-id*]

Parameter Description

Parameter	Description
process- id	OSPF process ID number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information about the OSPFv3 process.

```
FS# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
Enable two-way-maintain
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
LSA interval 5 secs, Minimum LSA arrival 1000 msecs
Pacing lsa-group: 30 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 11
Number of LSA received 4
Log Neighbor Adjency Changes : Enabled
Number of areas in this router is 2
Area BACKBONE(0)
Number of interfaces in this area is 1(1)
```

```
SPF algorithm executed 4 times
Number of LSA 3.    Checksum Sum 0x1DDF1
Number of Unknown LSA 0
  Area 0.0.0.1 (NSSA)
         Number of interfaces in this area is 1(1)
         SPF algorithm executed 5 times
         Number of LSA 7.    Checksum Sum 0x445FE
         Number of Unknown LSA 0
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
default-information originate	Sets the default route to be redistributed.
default-metric	Sets the default metric for the route to be redistributed.
router-id	Sets the OSPFv3 routing process ID
timers spf	Sets the delay and the minimum and maximum intervals for the OSPFv3 to perform SPF calculation after receiving the topology change information.

Platform Description

N/A

6.39 show ipv6 ospf database

Use this command to display the database information of the OSPFv3 process

show ipv6 ospf [*process- id*] **database** [**database-summary** | *lsa-type* [**adv-router** *router-id*]]

Parameter Description

Parameter	Description
process- id	OSPF process ID number
lsa-type	The LSA types are as follows: NSSA-external-LSA, AS-external-LSAs, Link-LSAs, Inter-Area-Prefix-LSAs, Inter-Area-Router-LSAs, Intra-Area-Prefix-LSAs, Network-LSAs, Router-LSAs If this parameter is not specified, all LSA information will be displayed.
adv-router *router-id*	Displays the LSA information generated by the specified router.
database-summary	Displays the LSA statistic information of OSPFv3 link status database.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

The following example displays the information about the OSPFv3 process database.

```
FS# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface FastEthernet 1/0)
Link State ID    ADV Router       Age  Seq#         CkSum    Prefix
0.0.0.2           1.1.1.1          197 0x80000001 0x7cd8        0
0.0.0.5           2.2.2.2          206 0x80000001 0x8c86        0
                  Link-LSA (Interface Loopback 1)
Link State ID    ADV Router       Age  Seq#         CkSum    Prefix
0.0.64.1          1.1.1.1           82 0x80000001 0xb760        0
                  Router-LSA (Area 0.0.0.0)
Link State ID    ADV Router       Age  Seq#         CkSum      Link
0.0.0.0           1.1.1.1        17 0x80000006 0x62a1         1
0.0.0.0           2.2.2.2          156 0x80000003 0x8653        1
                  Network-LSA (Area 0.0.0.0)
Link State ID    ADV Router       Age  Seq#         CkSum
0.0.0.5           2.2.2.2          157 0x80000001 0xf8f6
                  Router-LSA (Area 0.0.0.1)
Link State ID    ADV Router       Age  Seq#         CkSum      Link
0.0.0.0           1.1.1.1           17 0x80000002 0x0529        0
                  Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID    ADV Router       Age  Seq#         CkSum
0.0.0.1           1.1.1.1           77 0x80000002 0x83b4
AS-external-LSA
Link State ID    ADV Router       Age  Seq#         CkSum
0.0.0.1           1.1.1.1            1 0x80000001 0x6035 E2
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description N/A

6.40 show ipv6 ospf interface

Use this command to display the OSPFv3 interface information.

show ipv6 ospf [*process- id*] **interface** [*interface-type interface-number* | **brief**]

Parameter Description

Parameter	Description
interface-type interface-number	Specifies the interface type and interface number.

process- id	OSPFv3 process ID
brief	Displays the interface summary.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following example displays the information about the OSPFv3 interface.

```
FS# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (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 BDR, Priority 1
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

If the BFD has been enabled for the neighbor on the interface, the content of "BFD enabled" is also displayed. For example:

```
FS# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (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 BDR, Priority 1, BFD enabled
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.

Platform Description

N/A

6.41 show ipv6 ospf neighbor

Use this command to display the neighbor information of the OSPFv3 process.

show ipv6 ospf [*process- id*] **neighbor** [*interface-type interface-number* [**detail**] | *neighbor-id* | **detail** | **statistics**]

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number
detail	Displays details about the neighbor.
interface-type interface-number	Interface type and interface number
neighbor-id	Neighbor’s router ID
statistics	Displays the statistics of the neighbor.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following command displays the brief information about the OSPFv3 neighbor.

```
FS# show ipv6 ospf neighbor
OSPFv3 Process (1) , 1 Neighbors, 1 is Full:
Neighbor ID    Pri    State        Dead Time      Interface            Instance ID
2.2.2.2          1       Full/DR      00:00:33       FastEthernet 1/0    0
FS# show ipv6 ospf neighbor detail
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c
In the area 0.0.0.0 via interface FastEthernet 1/0
Neighbor priority is 1, State is Full, 6 state changes
```

```
DR is 2.2.2.2 BDR is 1.1.1.1
Options is 0x000013 (-|R|-|-|E|V6)
Dead timer due in 00:00:36
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
BFD session state up
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.
area virtual-link	Configures the OSPFv3 virtual link.
show ipv6 ospf interface	Displays the OSPFv3 interface information.

Platform Description

N/A

6.42 show ipv6 ospf restart

Use this command to display the OSPFv3 graceful restart configuration.

show ipv6 ospf [*process- id*] **restart**

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the restarter status.

```
FS# show ipv6 ospf restart
Routing Process is ospf 1
Graceful-restart enabled
Restart grace period 120 secs
Current Restart status is plannedRestart
Current Restart remaining time 50 secs
Graceful-restart helper support enabled
```

The following example displays the helper status.

```
FS# show ipv6 ospf restart
Routing Process is ospf 1
Neighbor 10.1.1.2, interface addr 10.1.1.2
In the area 0.0.0.0 via interface GigabitEthernet 6/0/0
Graceful-restart helper enabled
Current helper status is helping
Current helper remaining time 50 secs
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description

N/A

6.43 show ipv6 ospf route

Use this command to display the OSPFv3 route information.

show ipv6 ospf [*process- id*] **route** [**count**]

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number.
count	Total number of OSPFv3 routes

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the information about OSPFv3 routes.

```
FS# show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, 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 2Destination          Metric     Next-hop
E2 2001:DB8:1::/64     1/20      via fe80::c800:eff:fe84:1c, FastEthernet 1/0
O    2001:DB8:2::/64     11         via fe80::c800:eff:fe84:1c, FastEthernet 1/0, Area 0.0.0.0
```

Related Commands

Command	Description

ipv6 router ospf	Starts the OSPFv3 routing process.

Platform Description N/A

6.44 show ipv6 ospf summary-prefix

Use this command to display the external route convergence information of OSPFv3

show ipv6 ospf [*process- id*] **summary-prefix**

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the external route convergence information of OSPFv3.

```
FS# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix:
2001:db8::/64,Metric 16777215,Type0,Tag0,Match count0,advertise
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
summary-prefix	Configures the converge route outside the OSPFv3 routing domain.

Platform Description N/A

6.45 show ipv6 ospf topology

Use this command to display the topology information about each area of OSPFv3.

show ipv6 ospf [*process- id*] **topology** [**area** *area-id*]

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number
area-id	Area ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following command displays the topology information about each area of OSPFv3.

```
FS# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID         Bits    Metric        Next-Hop
Interface
1.1.1.1             EB    --
2.2.2.2             E      1              2.2.2.2
FastEthernet 1/0

OSPFv3 paths to Area (0.0.0.1) routers
Router ID         Bits    Metric        Next-Hop
Interface
1.1.1.1             B      --
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
area range	Configures the address range of the OSPF area.

Platform Description N/A

6.46 show ipv6 ospf virtual-links

Use this command to display the virtual link information of the OSPFv3 process

show ipv6 ospf [*process- id*] **virtual-links**

Parameter Description

Parameter	Description
process- id	OSPFv3 process ID number

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following command displays the information about the OSPFv3 virtual link.

```
FS# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 2.2.2.2 is down
   Transit area 0.0.0.1 via interface FastEthernet 1/0, instance ID 0
   Local address *
   Remote address 3333::1/128
   Transmit Delay is 1 sec, State Down,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in inactive
      Adjacency state Down
```

Related Commands

Command	Description
ipv6 router ospf	Starts the OSPFv3 routing process.
area virtual-link	Configures the OSPFv3 virtual link.
show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.

Platform Description

N/A

6.47 timers lsa arrival

Use this command to configure a delay for receiving repeated LSAs. Use the **no** form of this command to restore the default settings.

timers lsa arrival *arrival-time*

no timers lsa arrival

Parameter Description

Parameter	Description
arrival-time	Specifies the delay for receiving repeated LSAs. The range is from 0 to 600000 in the unit of milliseconds.

Defaults

The default is 1000.

Command Mode

Routing process configuration mode

Usage Guide

Configure the device not to process repeated LSAs received within the specific delay.

Configuration Examples

The following example sets the delay for receiving repeated LSAs to 2 seconds.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# timers lsa arrival 2000
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information, including identifiers of routing devices.

Platform Description

N/A

6.48 timers pacing lsa-group

Use this command to set an LSA group pace interval. Use the **no** form of this command to restore the default settings.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Parameter Description

Parameter	Description
seconds	Specifies the LSA group pace interval. The range is from 10 to 1800 in the unit of seconds. The default value is 30.

Defaults

The default is 30.

Command Mode

Routing process configuration mode

Usage Guide

Each LSA has its own lifetime, that is, LSA aging time. An LSA existing for 1800s will be refreshed so that the living time of the LSA will not exceed its aging time. This ensures that normal LSAs are not cleared due to timeout of aging time. If update and aging operations of each LSA are separately computed, a large number of CPU resources will be consumed.

To effectively utilize CPU resources, configure the device to group LSAs for uniform refreshment. The time for refreshing a group of LSAs is called an LSA group pace interval. Grouping refreshment is to put the LSAs to be refreshed within an LSA group pace interval into a group and refresh them uniformly.

When the number of LSAs is fixed, a longer LSA group pace interval will allow the CPU to process more LSAs when the timer expires for one time. To keep the stability of the CPU, you are recommended not to set an over long LSA group pace interval. This prevents the CPU from processing excessive LSAs when the timer expires each time. If the CPU processes a large number of LSAs each time, it is recommended to shorten the LSA group pace interval. For example, if the database has 10000 LSAs, you need to reduce the LSA group pace interval. If it has only 40 to 100 LSAs, you can adjust the group pace interval to 10 through 20 minutes.

Configuration Examples

The following example sets the LSA group pace interval to 120 seconds.

```
FS(config)# ipv6 router ospf 1
FS(config-router)#timers pacing lsa-group 120
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 configuration information.

Platform Description

N/A

6.49 timers pacing lsa-transmit

Use this command to set an interval for sending LSA groups. Use the **no** form of this command to restore the default settings.

timers pacing lsa-transmit *transmit-time transmit-count*

no timers pacing lsa-transmit

Parameter Description

Parameter	Description
transmit-time	Specifies the interval for sending LSA groups. The range is from 10 to 1000 in the unit of milliseconds.
transmit-count	Specifies the number of LS-UPD packets in an LSA group. The range is from 1 to 200.

Defaults

The default transmit-time is 40 and the transmit-count is 1.

Command Mode

Routing process configuration mode

Usage Guide

There are usually a lot of LSAs on a network; therefore, the load of the device is very high. Setting proper **transimit-time** and **transimit-count** values can restrict flooding of LS-UPD packets on the network.

When the CPU load is not high and network bandwidth usage is not large, you can reduce the **transimit-time** value and increase the **transimit-count** value to accelerate route convergence.

Configuration Examples

The following example sets the interval for sending LS-UPDs to 50 milliseconds and the specified 20 packets to be sent each time.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# timers pacing lsa-transmit 50 20
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information.

Platform Description

N/A

6.50 timers spf

Use this command to set the delay and interval for the OSPFv3 to calculate SPF after receiving the topology change. Use the **no** format of this command to restore the default settings.

timers spf *spf-delay holdtime*

no timers spf

Parameter Description

Parameter	Description
spf-delay	Defines the waiting time for the SPF calculation, which ranges from 0 to 2147483647 seconds. After receiving the topology change information, the OSPF routing process has to waiting for a given period before making the SPF calculation.
spf-holdtime	Defines the interval between two SPF calculations, which ranges from 0 to 2147483647 seconds. If the interval has not passed even if the waiting time has elapsed, no SPF calculation can be made yet.

Defaults

There are two default situations: 1. The versions earlier than FSOS 10.4 do not support the command **timers throttle spf**. The system default is timers spf 5 10. 2. The FSOS 10.4 and the later versions do support the command **timers throttle spf**, where **timer spf** takes no effect by default. The delay for SPF calculation is subject to the default settings of the command **timers throttle spf**. Refer to the description of the command.

Command Mode

Routing process configuration mode

Usage Guide

The smaller the *spf-delay* and *spf-holdtime*, the shorter time the OSPF takes to adapt to the topology change, but the more CPU time will be used of the router.

⚠ The **timer spf** configuration and the **timers throttle spf** configuration will overwrite each other.

Configuration Examples

The following example sets the delay and holdtime of the OSPFv3 to 3 seconds and 9 seconds respectively.

```
FS(config)# ipv6 router ospf 20
FS(config-router)# timers spf 3 9
```

Related Commands

Command	Description
clear ipv6 ospf	Restarts part of the function of the OSPFv3.
show ipv6 ospf	Displays the OSPFv3 routing process information.
timers throttle spf	Configures the exponential backoff delay of the SPF calculation

Platform Description

N/A

6.51 timers throttle lsa all

Use this command to configure an exponential backoff algorithm for generating LSAs. Use the **no** form of this command to restore the default settings.

timers throttle lsa all *delay-time hold-time max-wait-time*

no timers throttle lsa all

Parameter Description

Parameter	Description
delay-time	Specifies a shortest LSA generation delay, in milliseconds (the first batch of LSAs is usually generated immediately). The range is from 0 to 600000 in the unit of milliseconds.
hold-time	Specifies a shortest interval between the first two times of LSA refreshment, in milliseconds. The range is from 1 to 600000 in the unit of milliseconds
max-wait-time	Specifies a longest interval for consecutive two times of LSA refreshment, in milliseconds. The value is used to determine whether LSAs are refreshed consecutively. The range is from 1 to 600000 in the unit of milliseconds.

Defaults

The default *delay-time* is 0, *hold-time* is 5000 and *max-wait-time* is 5000.

Command Mode

Routing process configuration mode

Usage Guide

If high route convergence capability is needed when links are changed, set a small *delay-time* value.

To reduce CPU consumption, you can properly increase the values of the parameters.

The *hold-time* value cannot be smaller than the *delay-time* value and must be smaller than or equal to the *max-wait-time* value.

Configuration Examples

The following example sets *delay-time* to 10 milliseconds, *hold-time* to one second, and *max-wait-time* to five seconds.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# timers throttle lsa all 10 1000 5000
```

Related Commands

Command	Description
show ipv6 ospf	Displays OSPFv3 process information.

Platform Description

N/A

6.52 timers throttle route

Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the **no** form of this command to restore the default settings.

timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

no timers throttle route { **inter-area** | **ase** }

Parameter Description

Parameter	Description
inter-area	Calculates the inter area routes.
ia-delay	Sets the delay time of the inter-area route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the ia-delay time runs out.
ase	Calculates the external routes.
ase-delay	Sets the delay time of the external route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the ase-delay time runs out.

Defaults The default *ia-delay* is 0 and *ase-delay* is 0.

Command Mode Routing process configuration mode

Usage Guide The default settings are recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.

Configuration Examples The following example sets the delay time of the inter-area route calculation to one second.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# timers throttle route inter-area 1000
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

6.53 timers throttle spf

Use this command to configure, the delay for SPF calculation as well as the minimum and maximum intervals between two SPF calculations after receiving the topology change information for OSPFv3 in the routing process configuration mode. Use the **no** form of this command to restore the default settings.

timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

no timers throttle spf

Parameter Description

Parameter	Description
spf-delay	Specifies an SPF calculation delay after the topology change information is received. The range is from 1 to 600000 in the unit of milliseconds.
spf-holdtime	Specifies a shortest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.
spf-max-waittime	Specifies a longest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.

Defaults

The default *spf-delay* is 1000. *spf-holdtime* is 5000 and *spf-max-waittime* is 10000.

Command Mode

Routing process configuration mode.

Usage Guide

Spf-delay refers to the delay from the topology change to the SPF calculation. *Spf-holdtime* refers to the minimum interval between the first and the second SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval till it reaches to *spf-max-waittime*. If the interval between two SPF calculations has exceeded the required minimum value, the interval of SPF calculation will re-start from *spf-holdtime*.

Smaller *spf-delay* and *spf-holdtime* value can make the topology convergence faster. Greater *spf-max-waittime* value can reduce the SPF calculations. Those configuration are flexible according to the actual stability of the network topology.

Compared with the timers spf command, this command is more flexible. It not only speeds up the SPF convergence calculation, but also reduces the system resources consumption of SPF calculation as the topology changes continuously. Therefore, the timers throttle spf command is recommended.

ⓘ The spf-holdtime cannot be smaller than spf-delay, or the spf-holdtime will be set to be equal to spf-delay;

ⓘ The spf-max-waitime cannot be smaller than spf-holdtime, or the spf-max-waittime will be set to be equal to spf-holdtime automatically;

ⓘ The configuration of the timers spf command and of the timers throttle spf command are overwritten each other.

ⓘ With neither timers spf command nor timers throttle spf command configured, the default value refers to the default of the timers throttle spf command

Configuration Examples

The following example configures the delay and holdtime and the maximum time interval of the OSPFv3 as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the time for SPF calculation is: five milliseconds, one second, three seconds, seven seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90 seconds……

```
FS(config)# ipv6 router ospf 20
FS(config-router)# timers spf 5 1000 90000
```

Related Commands

Command	Description
clear ipv6 ospf	Restarts part of the OSPFv3 function.
show ipv6 ospf	Displays the routing process information of the OSPFv3
timers spf	Configures the SPF calculation delay .

Platform Description N/A

6.54 two-way-maintain

Use this command to enable two-way OSPFv3 maintenance. Use the **no** form of this command to disable this function.

two-way-maintain

no two-way-maintain

Parameter Description

Parameter	Description
N/A	N/A

Defaults Two-way OSPFv3 maintenance is enabled by default.

Command Mode Routing process configuration mode

Usage Guide Sometimes, there are a lot of sent and received packets on a network, occupying large CPU and memory resources. As a result, some packets cannot be processed immediately or are directly lost. If hello packets from a neighbor cannot be processed within the dead interval of neighbors, the connection with the neighbor will be interrupted due to connection timeout. If two-way OSPFv3 maintenance is enabled and a large number of packets exist on the network, besides hello packets, the two-way neighboring relationship between the device and the neighbor can also be maintained by DD, LSU, LSR, and LSAck packets from the neighbor. This prevents the neighboring relationship from failing due to receiving delay or discarding of hello packets.

Configuration Examples The following example disables two-way OSPFv3 maintenance.

```
FS(config)# ipv6 router ospf 1
FS(config-router)# no two-way-maintain
```

Related Commands

Command	Description
show ipv6 ospf	Displays global OSPFv3 configuration information.

Platform Description N/A

7 Protocol-independent Commands

7.1 accept-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its receiving direction. Use the no form of this command to restore the default value.

accept-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no accept-lifetime

Parameter description

Parameter	Description
start-time	Start time of the lifetime. The syntax is as follows: *hh:mm:ss month date year* *hh:mm:ss date month year* ● hh—hour ● mm—minute ● ss—second ● month—month ● date—day ● year—year The default start time is Jun 1, 1993, which is also the earliest start time available.
infinite	Indicates that the encryption key is valid for ever.
end-time	*End time of the encryption key. It must be later than the start time.*
duration ***seconds***	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

Default

infinite

Command mode

Encryption key configuration mode

Usage guideline

Use this command to specify the lifetime of an encryption key in its receiving direction.

Examples

The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011.

```
FS(config)# key chain ripkeys
FS(config-keychain)# key 1
FS(config-keychain-key)#accept-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011
```

Related command

Command	Description
-	-

Platform

-

description

7.2 ip as-path access-list

Use this command to configure an autonomous system (AS) path filter using a regular expression. Use the **no** form of this command to remove the AS path filter using a regular expression.

ip as-path access-list *path-list-num* { **permit** | **deny** } *regular-expression*

no ip as-path access-list *path-list-num* [{ **permit** | **deny** } *regular-expression*]

Parameter description

Parameter	Description
path-list-num	Specifies the AS-path access-list number. The range is from 1 to 500.
permit	Permits advertisement based on matching conditions.
deny	Denies advertisement based on matching conditions.
regular-expression	Regular expression that defines the AS-path filter. The expression length range is from 1 to 255 characters.

Default

By default, no AS path filter using a regular expression is configured.

Command mode

Global configuration mode

Usage guideline

N/A

Examples

The following example configures an AS path filter matching the path which contains AS number 123 only.

```
FS(config)# ip as-path access-list 105 deny ^123$
```

Related command

Command	Description
-	-

Platform description

-

7.3 ip community-list

Use this command to define a standard or expanded community list and control access to it. Use the **no** form of this command to remove the setting.

ip community-list { *community-list-number* **| standard** *community-list-name* } { **permit | deny** }
[{ *community-list-number* | **internet** | **local-AS**]

ip community-list { *community-list-number* | **expanded** *community-list-name* } { **permit | deny** }
[*regular-expression*]

Parameter

Parameter	Description

description

community-list-name	Name of the community list.
standard	Indicates standard community list numbered in 1 to 99.
expanded	Indicates expanded community list numbered in 100 to 199.
permit	Permits access to the community list.
deny	Denies access to the community list.
community-number	Community number in the form of AA:NN(AS number/2-byte numerical) in the range of 1 to 255 characters. It may also be one of the following value: Internet: Indicates the Internet community. All paths belong to this community. no-export: Indicates that this path will not be advertised to any EBGP peers. no-advertise: Indicates that this path will not be advertised to any BGP peers. local-as: Indicates that this path will not be advertised to out of the AS. When AS confederation is configured, this path will not be advertised to other ASs or sub-ASs.

Default configuration

None

Command mode

Global configuration mode.

Usage guidelines

Up to 32 community numbers are supported by each community, including **internet**, **local-AS**, **no-advertise** and **no-export.**

Examples

```
FS(config)# ip community-list standard 1 deny 100.20.200.20
FS(config)# ip community-list standard 1 permit internet
```

Related commands

Command	Description
match community	Match the community list.
set community-list delete	Remove the community value of the BGP path according to the community list.
show ip community-list	Show the community list information.

7.4 ip extcommunity-list

Use this command to create an extcommunity list and add an entry to the list. Use the **no** form of this command to remove the setting.

ip extcommunity-list {*expanded-list* | **expanded** *list-name* } { **permit | deny** } [*regular-expression*]

ip extcommunity-list {*standard-list* **| standard** *list-name* } { **permit | deny** } [**rt** *value*] [**soo** *value*]

Parameter description

Parameter	Description
expand-list	Indicates an extended extcommunity list, ranging from 100 to 199. One extcommunity list may contain multiple rules.
standard-list	Indicates a standard extcommunity list, ranging from 1 to 99. One extcommunity list may contain multiple rules.
expanded *list-name*	Indicates the name of an extended extcommunity, comprising not more than 32 characters. When using this parameter, you enter the extcommunity list configuration mode.
standard *list-name*	Indicates the name of a standard extcommunity list, comprising not more than 32 characters. When using this parameter, you enter the extcommunity list configuration mode.
permit	Defines an extcommunity rule for permitting.
deny	Defines an extcommunity rule for denying.
regular-expression	(optional) Defines a matching template that is used to match an extcommunity.
sequence-number	(Optional) Defines the sequence number of a rule, ranging from 1 to 2,147,483,647. If no sequence number is specified, the sequence number automatically increases by 10 when a rule is added by default. The initial number is 10.
rt	(Optional) Sets the RT attribute value. This command can be used only for the standard extcommunity configuration, but not for the extended extcommunity configuration.
soo	(Optional) Sets the SOO attribute value. This command can be used only for the standard extcommunity configuration, but not for the extended extcommunity configuration.
value	Indicates the value of an extended community (extend_community_value).

Default

It is disabled by default.

Command mode

Global configuration mode and ip extcommunity-list configuration mode.

Usage guidelines

This command is used to define the extcommunity list.

Examples

1.The following example defines an ip extcommunity-list.

```
FS(config)# ip extcommunity-list 1 permit rt 100：1
FS(config)# ip extcommunity-list standard aaa permit rt
100：2
FS(config)# ip extcommunity-list expanded ext1 permit 200：[0~9][0~9]
```

2. The following example displays how to use ip extcommunity.

```
FS(config)# route-map rt_in_filter
FS(config-route-map)# match extcommunity 1
FS(config-route-map)# match extcommunity ext1
FS(config)# router bgp 100
FS(config-router)# address-family vpn
FS(config-router-af)#neighbor 3.3.3.3 send-community extended
FS(config-router-af)#neighbor 3.3.3.3 route-map rt_in_filter in
```

7.5 ip prefix-list

Use this command to create a prefix list or add an entry to the prefix list. Use the **no** form of this command to remove the prefix list or an entry.

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

no ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*][**le** *maximum-prefix- length*]

Parameter description

Parameter	Description
prefix-list-name	Name of the prefix list
seq-number	Sequence number of an entry in the range of 1 to 2147483647. When you execute this command to add an entry without a sequence number, the system allocates a default sequence number for the entry. The default sequence number of the first entry is 5. Every subsequential entry without a sequence number uses the time of 5 larger than the previous sequence number as the default sequence number.
deny	Deny the route matching the prefix list.
permit	Permit the route matching the prefix list.
ip-prefix	Network address and mask. Network address can be any valid IP address and the mask length is in the range of 0 to 32.
minimum-prefix-length	(Optional) Minimum length of the prefix (the starting length) Note: “ge” indicates the operation of “larger than” and “equivalent to”.
maximum-prefix-length	(Optional) Maximum length of the prefix (the ending length) Note: “le” indicates the operation of “less than” and “equivalent to”.

Default configuration None

Command mode Global configuration mode.

Usage guidelines

The ip prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching.

You can execute this command to define an exact match, or use "ge" or "le" to define a range match for a prefix for flexible configuration. "ge" indicates the range of minimum-prefix-length to 32; "le" indicates the range of the mask length of the IP prefix to maximum-prefix-length; "ge" and "le" indicates the range of minimum-prefix-length to maximum-prefix-length, namely, mask length of IP prefix < minimum-prefix-length < maximum-prefix-length <=32.

Examples

The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 201.1.1.0/24.

```
FS# configure terminal
FS(config)# ip prefix-list pre1 permit 201.1.1.0/24
FS(config)# router ospf
FS(config-router)# distribute-list prefix pre1 out rip
FS(config-router)# end
```

7.6 ip prefix-list description

Use this command to add the description of a prefix list. Use the **no** form of this command to delete the description.

ip prefix-list *prefix-list-name* **description** *description-text*

Parameter description

Parameter	Description
prefix-list-name	Name of the prefix list
description-text	Description of the prefix list

Default configuration

No description is added for a prefix list, by default.

Command mode

Global configuration mode

Examples

The example below adds the description for the prefix list:

```
FS# configure terminal
FS(config)# ip prefix-list pre description Deny routes from Net-A
```

7.7 ip prefix-list sequence-number

Use this command to enable sort function for a prefix list. Use the **no** form of this command to disable the sort function.

ip prefix-list sequence-number

Parameter description

Disabled

Default configuration

No sequence number is added for a prefix list, by default.

Command mode

Global configuration mode

Examples

The example below adds a sequence number for the prefix list:

```
FS# configure terminal
FS(config)# ip prefix-list pre description deny routes from Net-A
```

Related commands

Command	Description
ip prefix-list	Configure the prefix list.

Platform description

N/A

7.8 key

Use this command to define an encryption key and enter the encryption key chain configuration mode. Use the no form of this command to delete it.

key *key-id*

no key *key-id*

Parameter description

Parameter	Description
key-id	Key ID, ranging from 0 to 2147483647.

Default

No encryption key is configured.

Command mode

Encryption key chain configuration mode.

Usage guideline

Use this command to define an encryption key.

Examples

The following example configures encryption key chain ripkeys and key 1.

```
FS(config)# key chain ripkeys
FS(config-keychain)# key 1
```

Related command

Command	Description
-	-

Platform description -

7.9 key chain

Use this command to define a key chain and enter the key chain configuration mode. Use the no form of this command to delete it.

key chain *key-chain-name*

no key chain *key-chain-name*

Parameter description

Parameter	Description
key-chain-name	Key chain name.

Default No key chain is configured.

Command mode Global configuration mode.

Usage guideline

⚠ For a key chain to take effect, you need to configure at least one key.

Examples The following example configures key chain ripkeys and enters the key chain configuration mode.

```
FS(config)# key chain ripkeys
```

Related command

Command	Description
-	-

Platform description -

7.10 key-string

Use this command to specify a key string. Use the no form of this command to delete it.

key-string [**0**|**7**] *text*

no key-string

Parameter description

Parameter	Description
0	Use plaintext.
7	Use encryption.
text	Authentication string.

Default No key string is configured.

Command mode Encryption key configuration mode.

Usage guideline

Use this command to specify a key string.

Examples

The following example configures key chain ripkeys, key 1 and the key string abc:

```
FS(config)# key chain ripkeys
FS(config-keychain)# key 1
FS(config-keychain-key)#key-string abc
```

Related command

Command	Description
-	-

Platform description

-

7.11 match community

Use this command to redistribute the routes matching the Community attribute permitted by the ACL in the route map configuration mode. Use the **no** form of this command to remove the setting.

match community { *community-list-number* | *community-list-name*} [**exact-match**] [{*community-list-number* | *community-list-name*} [**exact-match**] …]

no match community { *community-list-number* | *community-list-name*} [**exact-match**] [{ *community-list-number* | *community-list-name*} [**exact-match**] …]

Parameter description

Parameter	Description
community-list-number	Number of the standard community list in the range 1 to 99. Number of the extended community list in the range of 100 to 199
communitys-list-name	Name of the community list in the range of less than 80 characters
exact-match	Match the community list exactly.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

The match community can be followed by more than one community list number or name, but the total of community lists and names should not be greater than 6.

Each exact-match applies to only the previous list, not all the lists.

One or more match or set commands can be executed to configure one route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

```
FS(config)# ip community-list 1 permit 100:2 100:30
FS(config)# route-map set_lopref
FS(config-route-map)# match community 1 exact-match
FS(config-route-map)# set local-preference 20
```

Related commands

Command	Description
match as-path	Match the AS_PATH attribute.
match metric	Match the metric.
match origin	Match the source.
set as-path prepend	Set the AS_PATH attribute.
set metric	Set the metric.
set metric-type	Set the metric type.

7.12 match interface

Use **match interface** command to redistribute the routes whose next hop is the specified interface. Use the **no** form of this command to remove the setting.

match interface *interface-type interface-number* [*…interface-type interface-number*]

no match interface *[interface-type interface-number* [*…interface-type interface-number*]]

Parameter description

Parameter	Description
interface-type	Interface type
interface-number	Interface number

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

This command can be followed by multiple interfaces.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

The following example redistributes the RIP route with the next hop of fastethernet 0/0 in the OSPF routing protocol.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match interface fastethernet 0/0
```

Related commands

Command	Description
match ip address	Match the address in the access list.
match ip next-hop	Match the next-hop IP address in the access list.
match ip route-source	Match the source IP address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

7.13 match ip address

Use **match ip address** command to redistribute the routes matching the IP address permitted by the ACL or the prefix list. Use the **no** form of this command to remove the setting.

match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip address [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration None.

Command mode Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow match ip address.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

Examples

The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type-1 external type and the default metric being 40.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 200.168.23.0

route-map redrip permit 10
match ip address 10
set metric 40
set metric-type type-1!
```

Related commands

Command	Description
access-list	Set the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop address in the access list.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

7.14 match ip next-hop

Use **match ip next-hop** command to redistribute the routes whose next-hop IP address matches the access list or the prefix list. Use the **no** form of this command to remove the setting.

match ip next-hop {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]}

no match ip next-hop [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...*]]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list

prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers or names may follow match ip next-hop.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the next hop address of the RIP route matches the access list 10 or 20, the OSPF allows for redistribution.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 192.168.100.1
access-list 20 permit 172.16.10.1

route-map redrip permit 10
match ip next-hop 10 20
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

7.15 match ip route-source

Use **match ip route-source** command to redistribute the routes whose source IP address matches the access list.

Use the **no** form of this command to remove the setting.

match ip route-source {*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...]*}

no match ip route-source [*access-list-number* [*access-list-number...* | *access-list-name...*] |*access-list-name* [*access-list-number...*|*access-list-name*] | **prefix-list** *prefix-list-name [prefix-list-name...]*]

Parameter description

Parameter	Description
access-list-number	Number of the access list
access-list-name	Name of the access list
prefix-list *prefix-list-name*	Specify the prefix list to match.

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

Multiple access list numbers may follow match ip route-source.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the source IP address of the RIP route matches the access list 5, the OSPF allows for redistribution.

```
router ospf
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

access-list 5 permit 192.168.100.1

route-map redrip permit 10
 match ip route-source
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip next-hop	Match the next-hop IP address in the access list.
match metric	Match the metric.

match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

7.16 match length

Use this command to implement the policy-based routing based on the IP packet length in the route map configuration mode. The **no** form of Use this command to remove the setting.

match length *min-length max-length*

no match length *min-length max-length*

Parameter description

Parameter	Description
min-length	Minimum length of the IP packet
max-length	Maximum length of the IP packet

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Policy-based routing is a packet forwarding mechanism that is more flexible than the routing based on the destination network. After the policy-based routing is used, the device will decide how to process the packets needed to route according to the route map, which decides the next-hop device of the packets.

To apply the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

To route interactive traffic and mass traffic respectively, use the packet size based policy-based routing.

Examples

In the example below, the policy-based routing is enabled on fastethernet 1/0 to send the traffic with packet size smaller than 500 bytes through fastethernet 1/2 interface.

```
interface fastethernet 1/0
ip policy route-map smallpak

route-map smallpak permit 10
match length 0 500
set interface fastethernet 1/2
```

Related

Command	Description

commands

route-map	Define the route map
match ip address	Match the address in the access list
set default interface	Set the default packet output interface.
set interface	Set the packet output interface
set ip default next-hop	Set the default next hop of the packets.
set ip next-hop	Set the next-hop IP address of the packets
set ip precedence	Set the priority of the packets.

7.17 match metric

Use **match metric** command to redistribute the routes of the specified metric. Use the **no** form of this command to remove the setting.

match metric *metric*

no match metric *metric*

Parameter description

Parameter	Description
metric	Route metric, in the range 0 to 4294967295

Default configuration

None.

Command mode

Route map configuration mode.

Usage guidelines

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes of metric 10.

```
router ospf 1
redistribute rip subnets route-map redrip
network 192.168.12.0 0.0.0.255 area 0

route-map redrip permit 10
match metric 10
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.

match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

7.18 match route-type

Use this command to redistribute the network routes of the specified type. Use the **no** form of this command to delete the setting.

match route-type { **static** | **connect** | **rip** | **local** | **internal** | **external** [**type-1** | **type-2**] }

no match route-type [**static** | **connect** | **rip** | **local** | **internal** | **external** [**type-1** | **type-2**]]

Parameter description

Parameter	Description
local	Indicates the local route type.
static	Indicates the static route type.
connect	Indicates the directly connected route type.
rip	Indicates the RIP route type.
internal	Indicates the OSPF internal route type.
external	Indicates the OSPF external route type.
type-1 | type-2	Indicates the OSPF type-1 or type-2 route type.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the RIP routing protocol redistributes only the internal routes in the OSPF routing domain.

```
router rip
redistribute ospf route-map redrip
network 192.168.12.0
```

```
route-map redrip permit 10
match route-type internal
!
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the interface.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the access list.
set tag	Match the IP address.

7.19 match tag

Use this command to redistribute the network routes with the specified tag. Use the **no** form of this command to delete the setting.

match tag *tag* [… *tag*]

no match tag [*tag* [… *tag*]]

Parameter description

Parameter	Description
tag	Route tag

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

Multiple tags may follow the match tag command.

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the RIP routing protocol redistributes only the routes with tag 50 and 80 in the OSPF routing domain.

```
FS(config)# router rip
FS(config-router)# redistribute ospf 100 route-map redrip
FS(config-router)# network 192.168.12.0
FS(config-router)# exit
FS(config)# route-map redrip permit 10
FS(config-route-map)# match tag 50 80
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address.
match interface	Match the next-hop IP interface.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match ip next-hop	Match the next-hop IP address.
match route-type	Match the route type.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

7.20 memory-lack exit-policy

Use this command to configure a policy to preferentially exit a routing protocol when the memory reaches the lower limit. Use the **no** form of this command to restore the default policy, namely, exit the routing protocol which occupies the largest memory.

memory-lack exit-policy { **ospf** | **Rip** }

no memory-lack exit-policy

Parameter description

Parameter	Description
ospf	Preferentially exit OSPF when the memory is insufficient.
rip	Preferentially exit RIP when the memory is insufficient.

Default

By default, the routing protocol which occupies the largest memory exits preferentially.

Command mode

Global configuration mode

Usage guideline

When the memory reaches the lower limit, you can disable a routing protocol to release the memory to ensure the normal running of other protocols.

When the system runs out of memory, disable a routing protocol which has the minimal impact on the system to ensure the operation of main services.

Configuring the policy to preferentially exit the routing protocols which are disabled cannot help the system release memory.

This command ensures the operation of main services to some extent when the memory is insufficient. If the memory is further consumed, all routing protocols will exit and stop running.

Examples

Related command

Command	Description
-	-

Platform description

-

7.21 route-map

Use **route-map** to enter the route map configuration mode and define a route map. Use the **no** form of this command to remove the setting.

route-map *route-map-name* [**permit** | **deny**] [*sequence-number*]

no route-map *route-map-name* [{**permit** | **deny**}*sequence-number*]

Parameter description

Parameter	Description
route-map-name	Name of the route map. The redistribute command references the route map according to its name. Multiple routing policies can be defined in a route map, and each policy corresponds to one sequence number.
permit	(Optional) If the permit keyword is defined and the rule defined by match is met, The set command controls the redistributed routes. For policy-based routing, the set command controls the packet forwarding, and exits the route map operation. If the permit keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
deny	(Optional) If the deny keyword is defined and the rule defined by match is met, no operation will be performed. Neither route redistribution nor policy-based routing is supported in the route map. The system exits the route map operation. If the deny keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
sequence-number	Sequence number of the route map. The policy with a lower sequence number is preferred, so it's noted when setting the sequence number.

Default configuration

None.

Command mode

Global configuration mode.

Usage guidelines

At present, the FSOS software primarily uses the route map for route redistribution and policy-based routing.

1. Route redistribution control

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

When configuring route maps, pay attention to the following when using the sequence number of a route map:

When you create the first route map policy, if *sequence-number* is not specified, it is 10 by default;

If only one route map policy exists and *sequence-number* is not specified*,* no new route map policy will be created, and the existing route map policy will be accessed for configuration;

If more than one route map policy is available, the sequence number of each policy shall be specified; otherwise an error message will be displayed.

2. policy-based routing

Policy-based routing refers to a routing mechanism based on user defined policies. Compared with traditional destination IP address-based routing, policy-based routing offers a flexibility for routing based on source IP address, length and port of IP packets. Policy-based routing can apply to the IP packets received on an interface or the IP packets sent from the local device.

Policy-based routing utilizes route map to define routing and forwarding policy. The match command defines packet filtering rule and the set command defines the action for the packets matching the filtering rules. The match command used includes match ip address and match length; the set command includes set ip tos, set ip precedence, set ip dscp, set ip [default] nexthop, set ip next-hop verify-availability, set [default] interface.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes with the hop count of 4. In the OSPF route domain, the route type is the external route type-1, the default metric is 40 and the tag is 40.

```
!
router ospf
  redistribute rip subnets route-map redrip
  network 192.168.12.0 0.0.0.255 area 0
!
!
route-map redrip permit 10
  match metric 4
  set metric 40
  set metric-type type-1
set tag 40
```

Related commands

Command	Description
redistribute	Redistribute the routes.

7.22 send-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its send direction. Use the no form of this command to restore the default value.

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime

Parameter description

Parameter	Description
start-time	Start time of the lifetime.
infinite	Indicates that the encryption key is valid for ever.
end-time	*End time of the encryption key. It must be later than the start time.*
duration *seconds*	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.

Default

infinite

Command mode

Encryption key configuration mode

Usage guideline

Use this command to specify the lifetime of an encryption key in its send direction.

Examples

The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011

```
FS(config)# key chain ripkeys
FS(config-keychain)# key 1
FS(config-keychain-key)# send-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011
```

Related command

Command	Description
-	-

Platform description

-

7.23 set default interface

Use this command to specify the default interface for forwarding the packets whose route matches the rule but without an egress in the route map configuration mode. Use the **no** form of this command to remove the setting.

set default interface *interface-type interface-number* […*interface-type interface-number*]

no set default interface *interface-type interface-number* […*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Interface type.
interface-number	Interface number.

Default

None

Command mode

Route map configuration mode

Usage guideline

Multiple interfaces may follow the set default interface command.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the device will determine how to process the packets to be routed according to the route map, which determines the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

If the first defined interface becomes down, the interface set by the second set command will be attempted. A route-map policy may contain multiple set operations.

Examples

In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic whose packet size is less than 500 bytes and the route is not defined through fastEthernet 1/0 interface.

```
FS(config)# interface serial 1/0
FS(config-if)# ip policy route-map smallpak
FS(config-if)# exit
FS(config)# route-map smallpak permit 10
FS(config-route-map)# match length 0 500
FS(config-route-map)# set default interface fastethernet 1/0
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
match length	Match the packet length.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop of the packets.
set ip next-hop	Set the next-hop IP address of the packets.
set ip precedence	Set the priority of the packets.

7.24 set interface

Use this command to specify the interface for forwarding the packets matching the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set interface *interface-type interface-number* […*interface-type interface-number*]

no set interface *interface-type interface-number* […*interface-type interface-number*]

Parameter description

Parameter	Description
interface-type	Interface type.
interface-number	Interface ID

Default None

Command mode Route map configuration mode

Usage guideline

Multiple interfaces may follow the set interface command.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. If policy-based routing is used, the device will determine how to process the packets to be routed according to the route map, which determines the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

If the first defined interface becomes down, the interface set by the second set command will be attempted. A route-map policy may contain multiple set operations.

If the interface is set as null 0, the packets will be discarded.

Examples

In the example below, the policy-based routing is enabled on serial 1/0 to send the traffic whose packet size is less than 500 bytes through fastethernet 0/0 interface.

```
FS(config)#interface serial 1/0
FS(config-if)#ip policy route-map smallpak
FS(config)#route-map smallpak permit 10
FS(config-route-map)#match length 0 500
FS(config-route-map)#set interface fastethernet 0/0
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
match length	Match the packet length.
set default interface	Set the default outgoing interface when there is no route in the routing table.
set ip default next-hop	Set the default next hop of the packets when there is no route

	in the routing table.
set ip next-hop	Set the next-hop IP address of the packets.
set ip precedence	Set the priority of the packets.

Platform description

This command is not supported on switches, but supported on the routers.

7.25 set ip default next-hop

Use this command to specify the default next-hop IP address for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip default next-hop *ip-address* [*weight*] […*ip-address* [*weight*]]

no set ip default next-hop [*ip-address* [*weight*] […*ip-address* [*weight*]]]

Parameter description

Parameter	Description
ip-address	IP address of the next hop.
weight	Weight of the next hop.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight inputted.

Up to 32 IP addresses may follow the **set ip default next-hop** command.

If a weight follows ip address, up to 4 next hop IP addresses can be configured.

⚠ If a weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In this mode, the weight of those next hop IP addresses whose weight is not configured is 1 by default.

Differences between set ip next-hop and set ip default next-hop: After the set ip next-hop command is configured, the policy-based routing takes precedence over the routing table; while after the set ip default next-hop command is configured, the routing table takes precedence over the policy-based routing.

Use this command to customize a default route for a specified user. If the software fails to find the forwarding route, the packet will be forwarded to the nexthop set with this command.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded through the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

Examples

The following example forwards the packets from two different nodes through different routes.

For the messages received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding route, they are forwarded to device 6.6.6.6. For the messages received from 2.2.2.2, if the software cannot find the forwarding route, they are forwarded to device 7.7.7.7. The other messages will be discarded if the software cannot find the forwarding route.

```
FS(config)#access-list 1 permit 1.1.1.1 0.0.0.0
FS(config)#access-list 2 permit 2.2.2.2 0.0.0.0
FS(config)#interface async 1
FS(config-if)#ip policy route-map equal-access
FS(config)#route-map equal-access permit 10
FS(config- route-map)#match ip address 1
FS(config-route-map)#set ip default next-hop 6.6.6.6
FS(config)#route-map equal-access permit 20
FS(config-route-map)#match ip address 2
FS(config-route-map)#set ip default next-hop 7.7.7.7
FS(config)#route-map equal-access permit 30
FS(config- route-map)#set default interface null 0
```

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

Platform description

N/A

7.26 set ip dscp

Use this command to specify the DSCP value for the packets that match the rule in the route map configuration mode. Use the **no** form of this command to remove the setting.

set ip dscp *dscp-value*

no set ip dscp

Parameter description

Parameter	Description
dscp-value	DSCP value

Default configuration

N/A

Command

Route map configuration mode

mode

Usage guideline N/A

Examples N/A

Related commands

Command	Description
route-map	Define a route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip next-hop	Set the next hop of the packets.
set ip precedence	Set the priority of the packets.

7.27 set ip next-hop

Use this command to specify the next-hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop *ip-address* [*weight*] […*ip-address* [*weight*]]

no set ip next-hop [*ip-address* [*weight*] […*ip-address* [*weight*]]]

Parameter description

Parameter	Description
ip-address	Indicates the next-hop IP address.
weight	Indicates the weight of this next hop.

Default configuration None

Command mode Route map configuration mode

Usage guideline

This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user. Multiple IP addresses may follow set ip next-hop and the number of addresses should be less than 32.

If a weight follows ip address, up to 4 next hop IP addresses can be configured.

⚠ If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

This command can be used to set different routes for the traffic that meets different match rule. If multiple IP addresses are configured, they can be used in turn.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. After the policy-based routing is used, the device will decide how to process the packets that need be routed according to the route map, which decides the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

Examples

The following example enables policy-based routing on serial 1/0. When the interface receives the packets from 10.0.0.0/8, they will be sent to 192.168.100.1; when the interface receives the packets from 172.16.0.0/16, they will be sent to 172.16.100.1; all other packets will be discarded.

```
FS(config)#interface serial 1/0
FS(config-if)#ip policy route-map load-balance
FS(config)#access-list 10 permit 10.0.0.0 0.255.255.255
FS(config)#access-list 20 permit 172.16.0.0 0.0.255.255
FS(config)#route-map load-balance permit 10
FS(config-route-map)#match ip address 10
FS(config-route-map)#set ip next-hop 192.168.100.1
FS(config)#route-map load-balance permit 20
FS(config-route-map)#match ip address 20
FS(config-route-map)#set ip next-hop 172.16.100.1
FS(config)#route-map load-balance permit 30
FS(config-route-map)#set interface Null 0
```

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

7.28 set ip next-hop verify-availability

Use this command to verify the availability of the next hop IP address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ip next-hop verify-availability *ip-address* **track** *track-object-num*

no set ip next-hop verify-availability *ip-address* [**track** *track-obj-number*]

Parameter

Parameter	Description

description

ip-address	Indicates the next-hop IP address.
track	Judges whether the next hop is effective by using *Track*.
track-object-num	Indicates the track object number.

Default configuration None

Command mode Route map configuration mode

Usage guideline None

Examples

The following example verifies the availability of the next hop IP address being 192.168.1.2 and the number of the object to be tracked to 1.

```
FS(config)#route-map rmap permit 10
FS(config-route-map)#set ip next-hop verify-availability 192.168.1.2 track 1
```

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

7.29 set ip precedence

Use this command to set the precedence of the IP head of the packet matching the rule in the route map configuration mode. Use the **no** form of this command to remove the configured precedence setting.

set ip precedence {*<0-7>* | *critical* | *flash* | *flash-override* | *immediate* | *internet* | *network* | *priority* | *routine* }

no set ip precedence

Parameter Description

Parameter	Description
number	Indicates the priority of the IP header with a number, ranging from 0 to 7. 7: critical 6: flash 5: flash-override 4: immediate 3: internet 2: network 1: priority

	0: routine
critical | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**	Priority of an IP header.

Defaults

N/A

Command mode

Route map configuration mode

Usage guideline

With different precedence values for the IP packet head configured, the IP packets matching the PBR routing are sent according to the different precedence values.

Multiple set ip precedence commands can be executed in the route map configuration rule, but only the last one takes effect, and the precedence will be specified for the head of the IP packet matched the PBR.

Examples

The following example sets the precedence of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:

```
FS(config)#access-list 1 permit 192.168.217.68 0.0.0.0
FS(config)#route-map name
FS(config-route-map)#match ip address 1
FS(config-route-map)#set ip precedence 4
FS(config)#interface FastEthernet 0/0
FS(config-if)#ip policy route-map name
```

Related commands

Command	**Description**
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip tos	Set the tos for the IP packet head.

7.30 set ip tos

Use this command to set the tos of the IP head of the packet matching the rule in the route map configuration mode. Use the **no** form of this command to remove the configured tos setting.

set ip tos {*<0-15>* | *max-reliability* | *max-throughput* | *min-delay* | *min-monetary-cost* | *normal* }

no set ip tos

Parameter

Parameter	**Description**

Description

number	Indicates the TOS value of an IP header with a number, ranging from 0 to 15. 2: **max-reliability** 4: **max-throughput** 8: **min-delay** 1: **min-monetary-cost** 0: **normal**
max-reliability | max-throughput | min-delay | min-monetary-cost | normal	Priority of an IP header.

Defaults N/A

Command mode Route map configuration mode

Usage guideline

With different TOS values for the IP packet head configured, the IP packets matching the PBR routing are transmitted with different service qualities.

The TOS value will be specified for the head of the IP packet matched the PBR.

Examples

The following example sets the TOS value of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4:

```
FS(config)#access-list 1 permit 192.168.217.68 0.0.0.0
FS(config)#route-map name
FS(config-route-map)#match ip address 1
FS(config-route-map)#set ip tos 4
FS(config)#interface FastEthernet 0/0
FS(config-if)#ip policy route-map name
```

Related commands

Command	Description
match interface	Match the next-hop interface.
match ip address	Match the IP address in the ACL.
match ip next-hop	Match the next-hop IP address in the ACL.
match ip route-source	Match the route source IP address in the ACL.
match metric	Match the route metric value.
match route-type	Match the route type.
match tag	Match the route tag value.
set metric-type	Set the type of redistributed route.
set tag	Set the tag value of redistributed route.
set ip precedence	Set the precedence for the IP packet head.

7.31 set level

Use this command to set the level of the area where the routes matching the rule are redistributed in the route map configuration command. Use the **no** form of this command to remove the setting.

set level {stub-area | backbone}

no set level

Parameter Description

Parameter	Description
stub-area	Indicates that the re-distribution route is advertised to OSPF Stub Area.
backbone	Indicates that the re-distribution route is advertised to the OSPF backbone area.

Default configuration None

Command mode Route map configuration mode

Examples

In the example below, the OSPF routing protocol redistributes the RIP protocol to the backbone area.

```
FS(config)# router ospf
FS(config-router)# redistribute rip subnets route-map redrip
FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
FS(config-router)# exit
FS(config)# route-map redrip permit 10
FS(config-route-map)# set level backbone
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

7.32 set metric

Use **set metric** to set the metric for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric [+ *metric-value* | **-** *metric-value* | *metric-value*]

no set metric

Parameter

Parameter	Description

description

+	Increase based on the metric of the original route
-	Decrease based on the metric of the original route
metric-value	Metric for the route to be redistributed

Default configuration

The default metric for route redistribution varies with the routing protocol.

Command mode

Route map configuration mode

Usage guideline

You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attentions should be paid to the upper and lower limits of the routing protocols when you execute the set metric, + metric or – metric commands. When the RIP protocol redistributes the routes of other protocols, the range of the metric after increase or decrease is 1 to 16.

You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes and sets the default metric to 40.

```
FS(config)# router ospf
FS(config-router)# redistribute rip subnets route-map redrip
FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
FS(config-router)# exit
FS(config)# route-map redrip permit 10
FS(config-route-map)# set metric 40
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

7.33 set metric-type

Use **set metric-type** to set the type of the routes to be redistributed. Use the **no** form of this command to remove the setting.

set metric-type *type*

no set metric-type

Parameter description

Parameter	Description
type	Type of the routes to be redistributed. At present, you can set the type of the routes that the OSPF protocol redistributes. type-1: Type-1 external route; type-2: Type-2 external route.

Default configuration Type-2

Command mode Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the type as type-1.

```
FS(config)# router ospf
FS(config-router)# redistribute rip subnets route-map redrip
FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
FS(config-router)# exit
FS(config)# route-map redrip permit 10
FS(config-route-map)# set metric-type type-1
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.

set metric	Set the metric.
set tag	Set the tag.

7.34 set next-hop

Use this command to specify the next-hop IP address for the routes that match the rule. Use the **no** form of this command to remove the setting. This command is only used to configure routing policies.

set next-hop *ip-address*

no set next-hop

Parameter description

Parameter	Description
ip-address	IP address of the next hop.

Default configuration

None

Command mode

Route map configuration mode

Usage guideline

You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.

In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the next-hop to 192.168.1.2.

```
FS(config)# route-map redrip permit 10
FS(config-route-map)# match ip address 1
FS(config-route-map)# set next-hop 192.168.1.2
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric-type	Set the metric type.
set tag	Set the tag.

7.35 set tag

Use this command to set the tag for the routes to be redistributed. Use the **no** form of this command to remove the setting.

set tag *tag*

no set tag

Parameter description

Parameter	Description
tag	Tag of the route to be redistributed

Default configuration

The original routing tag remains unchanged.

Command mode

Route map configuration mode

Usage guideline

This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP route and sets the tag as 100.

```
FS(config)# router ospf
FS(config-router)# redistribute rip subnets route-map redrip
FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
FS(config-router)# exit
FS(config)# route-map redrip permit 10
FS(config-route-map)# set tag 100
```

Related commands

Command	Description
match interface	Match the interface.
match ip address	Match the IP address.
match ip next-hop	Match the next-hop IP address.
match ip route-source	Match the source IP address.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.

7.36 show ip as-path-access-list

Use this command to display the configuration of AS path access lists.

show ip as-path-access-list [*num*]

Parameter description

Parameter	Description
num	AS path access list number.

Default

N/A

Command mode

Privileged EXEC mode

Usage guideline

N/A

Examples

The following example displays the AS path access lists.

```
FS# show ip as-path-access-list
AS path access list 30
permit ^30$
```

Field	Description
AS path access list	AS path access list number
permit	Permits advertisement based on matching conditions.
^30$	Regular expression.

Related command

Command	Description
-	-

Platform description

-

7.37 show ip community-list

Use **show ip community-list** command to display the community list.

show ip community-list [*community-list-number* | *community-list-name*]

Parameter description

Parameter	Description
community-list-number	Number of the community list.
community-list-name	Name of the community list.

Default configuration

None

Command mode

Privileged EXEC mode

Usage guidelines

N/A

Examples

```
FS# show ip community-list
Community-list standard local
permit local-AS
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

Related commands

Command	Description
match community	Match the route community.
set comm-list delete	Delete the community attribute in the BGP routes.

7.38 show ip extcommunity-list

Use this command to display the extcommunity list.

show ip extcommunity-list [*extcommunity-list-num* | *extcommunity-list-name*]

Parameter description

Parameter	Description
extcommunity-list-num	extcommunity-list number, ranging from 1 to 199.
extcommunity-list-name	extcommunity-list name.

Default

-

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode and route map configuration mode.

Usage guideline

-

Examples

```
FS # show ip extcommunity-list
Standard extended community-list 1
  10 permit RT:1:200
  20 permit RT:1:100
Standard extended community-list 2
  10 permit RT:1:200
Expanded extended community-list rt_filter
  13 permit 1:100
```

Related command

Command	Description
ip extcommunity-list	Create an extcommunity-list.
match extcommunity	Match an extcommunity.

set extcommunity	Set an extcommunity.

Platform description

-

7.39 show ip prefix-list

Use **show ip prefix-list** to display the prefix list or the entries.

show ip prefix-list [*prefix-name*]

Parameter description

Parameter	Description
prefix-name	Name of the prefix list.

Default configuration

The configuration information of all the prefix lists is displayed by default.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples

```
FS# show ip prefix-list
seq pre: 2 entries
seq 5 permit 192.168.564.0/24
seq 10 permit 192.2.2.0/24
```

7.40 show ip protocols

Use this command to display information about the status of the currently running IPv4 routing protocol.

show ip protocols { **Ospf | Rip** }

Parameter Description

Parameter	Description
ospf	Displays information about the status of the OSPF protocol.
rip	Displays information about the status of the RIP protocol.
-	Displays information about the status of all running routing protocols.

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and routing map configuration mode

Default Level

14

Usage Guide Information about the status of only the currently running routing protocol is displayed, and the information about a routing protocol that is not running is not displayed.

Examples N/A

7.41 show key chain

Use this command to display the key chain configuration.

show key chain [*key-chain-name*]

Parameter description

Parameter	Description
key-chain-name	(Optional) Display the configuration of the specified key chain.

Default The configuration information of all key chains is displayed.

Command mode Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and key chain configuration mode.

Usage guideline If no key chain is specified, the configuration information of all key chains is displayed.

Examples

```
FS# show key chain
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
FS(config)#show key chain
key chain kc
    key 1 -- text "FS"
        accept-lifetime (12:11:00 May    2 2001) - (infinite)
        send-lifetime (always valid) - (always valid) [valid now]
```

Field	Description
key chain	Key chain name.
key	Key ID.
text	Key string.
accept-lifetime	Lifetime in the accept direction.
send-lifetime	Lifetime in the send direction.

Related command

Command	Description
-	-

Platform description

-

7.42 show route-map

Use the command to display the configuration of the route map.

show route-map [*route-map-name*]

Parameter description

Parameter	Description
route-map-name	(Optional) Display the configuration information of the specified the route map.

Default configuration

The configuration information of all the route maps is displayed.

Command mode

Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines

If no route map is specified, the configurations of all the route maps will be displayed, otherwise only the configuration of the specified route map is displayed.

```
FS# show route-map
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
```

Examples

Field	Description
route-map	Name of the route map.
Permit	The route map contains the permit keyword.
sequence 10	Sequence number of the route map.
Match clauses	Set the matching rule. Whether to perform the set operation depends on the permit or deny keyword in the route map.
Set clauses	Set the operation when the rule is matched.

8 NSM Commands

8.1 clear ip route

Use this command to clear the route cache.

clear ip route { * **|** *network* [*netmask*] | }

Parameter Description

Parameter	Description
*	Clears all route cache.
network	Specifies the route cache of the network or subnet.
netmask	(Optional) Subnet mask. If no subnet mask is specified, the longest match principle is used when you match *network* with the route. The cache of the longest match is cleared.

Command Mode Privileged EXEC mode

Usage Guide Clearing route cache clears the corresponding routes and triggers the routing protocol relearning. Please note that clearing all route cache leads to temporary network disconnection.

Examples The following example clears the cache of the route which is the longest match with IP address 192.168.12.0.

```
clear ip route 192.168.12.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

8.2 ip default-gateway

Use this command to configure the default gateway IP address on 2-layer devices. Use the **no** or **default** form of this command to restore the default setting.

ip default-gateway *ip-address*

no ip default-gateway

default ip default-gateway

Parameter Description

Parameter	Description
ip-address	IPv4 address of the default gateway

Defaults No gateway IP address is configured by default.

Command Mode Global configuration mode

Usage Guide When the device does not know the destination address of a packet, the device will forward the packet to the default gateway.

This command is supported on 2-layer devices. And it is also supported on 3-layer devices after the **no ip routing** command is applied.

Examples The following example sets the IP address of default gateway to 192.168.1.1.

```
ip default-gateway 192.168.1.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

8.3 ip default-network

Use this command to configure the default network globally. Use the **no** or **default** form of this command to restore the default setting.

ip default-network *network*

no ip default-network *network*

default ip default-network *network*

Parameter Description

Parameter	Description
network	Default network

Defaults The default is 0.0.0.0/0.

Command Mode Global configuration mode

Usage Guide The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network.

The default network always starts with an asterisk ("*"), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a static route.

Examples The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.

```
ip route 192.168.100.0 255.255.255.0 serial 0/1
ip default-network 192.168.100.0
```

The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.

```
ip default-network 200.200.200.0
```

Related Commands

Command	Description
show ip route	Displays the routing table.

8.4 ip route

Use this command to configure a static route. Use the **no** or **default** form of this command to restore the default setting.

ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent | {track** *object-numbe* **}**] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**]

no ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*]

no ip route all

default ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*]

Parameter Description

Parameter	Description
network	Network address of the destination
net-mask	Mask of the destination
ip-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
distance	(Optional) The administrative distance of the static route
tag	(Optional) The tag of the static route
permanent	(Optional) Permanent route ID
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

No static route is configured by default.

Command Mode

Global configuration mode

Usage Guide

The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

The default weight of the static route is 1. To view the static route of non default weight, execute the **show ip route weight** command. The parameter weight is used to enable WCMP. When there are load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flow the route carries. WCMP limit is generally 32 for routers. However, WCMP limit varies by switch models for their chipsets support different weights. When the sum of the weights of load balanced routes is beyond this weight limit, the excessive ones will not take effect.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it.

When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, ip route 0.0.0.0 0.0.0.0 Fastethernet 0/0. In this case, the switch may consider that all unknown destination networks are directly connected to the Fastethernet 0/0. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not recommended to set the static route to an Ethernet interface.

Association between a static route and a track object can be specified. When association between a static route and a specified track object is configured and the advertised track object status is inactive, the static route does not take effect. If the advertised track object status is active, the static route takes effect based on another status. With association between a static route and a track object, the third-party status concerned by the track object is mainly used to determine whether the static route takes effect. Association between a static route and a track object cannot be used for routes with the permanent attribute.

Examples

The following example adds a static route to the destination network of 172.16.100.0/24 whose next hop is 192.168.12.1 and administrative distance is 15.

```
ip route 172.16.199.0 255.255.255.0 192.168.12.1 155
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures data flows to be sent through fastehternet 0/0 to the destination network of 172.16.100.0/24.

```
ip route 172.16.199.0 255.255.255.0 fastethernet 0/0 192.168.12.1
```

Related Commands

8.5 ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** or **default** form of this command to disable this function.

ip routing

no ip routing

default ip routing

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

IP routing is not necessary when the switch serves as bridge or VoIP gateway.

When a device functions only as a bridge or VoIP gateway, the IP routing function of the FSOS software is not required. In this case, the IP routing function of the FSOS software can be disabled.

After the IP routing function is disabled, the device functions as a common host. The device can send and receive packets but cannot forward packets. All route-related configurations will be deleted except the static route configuration. A large number of static routes may be configured. If a user runs the **no ip routing** command, the configuration of a large number of static routes may be lost. To prevent this situation, the static route configuration will be hidden temporarily when the **no ip routing** command is run. If the **ip routing** command is run again, the static route configuration can be restored.

Note that if the process or whole system restarts when the **no ip routing** command is run, the static route configuration will not be reserved.

Examples

The following example disables IP routing.

```
FS(config)# no ip routing
```

Related Commands

N/A

Platform Description

8.6 ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

ip static route-limit *number*

no ip static route-limit *number*

default ip static route-limit

Parameter Description

Parameter	Description
number	Upper threshold of static routes in the range from 1 to 10000

Defaults

The default is 1024.

Command Mode

Global configuration mode

Usage Guide

The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the **show running-config** command.

Examples

The following example sets the upper threshold of the static routes to 900 and then restores the setting to the default value.

```
ip static route-limit 900
```

Related Commands

N/A

Platform Description

8.7 ipv6 default-gateway

Use this command to configure the default gateway IPv6 address on 2-layer devices. Use the **no** or **default** form of this command to restore the default setting.

ipv6 default-gateway *ipv6-address*

no ipv6 default-gateway

default ipv6 default-gateway

Parameter Description

Parameter	Description
ipv6-address	Sets the default gateway IPv6 address.

Defaults

No gateway IPv6 address is configured by default.

Command Mode

Global configuration mode

Usage Guide

When the device does not know the destination address of a packet, the device will forward the packet to the default gateway. Use the command **show ipv6 redirects to** display default gateway configuration.

Examples

The following example sets the default gateway IPv6 address to 10::1.

```
FS(config)# ipv6 default-gateway 10::1
```

Platform Description

This command is not supported on 2-layer devices or 3-layer devices configured with the **no ip routing** command.

8.8 ipv6 route

Use this command to configure an ipv6 static route. Use the **no** or **default** form of this command to restore the default setting.

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*] [**tag** *tag*] [**weight** *number*] [**description** *description-text*]

no 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*]

no ipv6 route [**vrf** *vrf_name*] **all**

Parameter

Parameter	Description

Description

vrf *vrf-name*	Name of VRF, which must be the configured IPv6 address family multi-protocol VRF
prefix-length	Mask length of the destination
ipv6-address	The next hop IP address of the static route
interface	(Optional) The next hop egress of the static route
nexthop-vrf *vrf-name1*	(Optional) VRF the nexthop belongs, which must be the configured IPv6 address family multi-protocol VRF.
distance	(Optional) The administrative distance of the static route. The default is 1.
tag	(Optional) The tag value of the static route. The default is 0.
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*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.

Defaults

No IPv6 static route is configured by default.

Command Mode

Global configuration mode

Usage Guide

When the multi-protocol VRF deletes the IPv6 address family, the IPv6 static route of VRF that the route or nexthop belongs is deleted.

If the VRF of the IPv6 static route interface is not same as the nexthop's VRF, then this IPv6 static route takes no effect.

The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

Examples

The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance are 115.

```
ipv6 route 2001::/64 2002::2 115
```

If the static route has not a specific interface, data flows may be sent thought other interface in case of interface failure. The following example configures that data flows are sent through fastehternet 0/0 to the destination network of 2001::/64.

```
ipv6 route 2001::/64 fastethernet 0/0 2002::2
```

Related Commands

Command	Description
show ipv6 route	Displays IPv6 routing table.

Platform Description

This command is not supported on 2-layer devices.

8.9 ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

Ipv6 static route-limit { number | **default-vrf** *number* | **vrf** *vrf-name number* }

no ipv6 static route-limit [**default-vrf**] | [**vrf** *vrf-name*]

default ipv6 static route-limit [**default-vrf**] | [**vrf** *vrf-name*]

Parameter Description

Parameter	Description
number	Upper threshold of static routes in the range from 1 to 1,000,000.
default-vrf *number*	Upper threshold of static routes in the range from 1 to 10,000 in default VRF scenario.
vrf *vrf-name number*	Upper threshold of static routes in the range from 1 to 10,000 in VRF scenario.

Defaults

The default is 1000.

Command Mode

Global configuration mode

Usage Guide

The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the show running config command.

Examples

The following example sets the upper threshold of the global static routes to 900, the upper threshold of the global static routes to 200 in default VRF scenario, the upper threshold of the global static routes to 100 in VRF scenario and then restores the setting to the default value.

```
FS(config)#ipv6 static route-limit ?
  <1-1000000>   Global limit value(default value: 1024)

  default-vrf   Default Routing/Forwarding instance

  vrf           VPN Routing/Forwarding instance

FS(config)# ipv6 static route-limit 900

FS(config)# ipv6 static route-limit default-vrf   200
FS(config)# ipv6 static route-limit vrf test 100


FS(config)# no ipv6 static route-limit


FS(config)# no ipv6 static route-limit default-vrf
FS(config)# no ipv6 static route-limit vrf test
```

Related Commands

Command	Description
ipv6 route	Configures the IPv6 static route.
show ipv6 route	Displays the IPv6 routing table.

Platform Description

This command is not supported on 2-layer devices.

8.10 ipv6 unicast-routing

Use this command to enable the IPv6 route function of the FSOS. Use the **no** or **default** form of this command to disable this function.

ipv6 unicast-routing

no ipv6 unicast-routing

default ipv6 unicast-routing

Parameter Description

N/A

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

This function can be disabled if the device is just used as the bridge-connection device or the VOIP gateway device.

Examples

The example disables the IPv6 route function of FSOS.

```
FS# no ipv6 unicast-routing
```

Related Commands

Command	Description
ipv6 route	Configure the IPv6 static route.
show ipv6 route	Displays the IPv6 routing table.

Platform

This command is not supported on 2-layer devices.

Description

8.11 maximum-paths

Use this command to specify the number of equivalent routes. Use the **no** or **default** form of this command is used to restore the default setting.

maximum-paths *number*

no maximum-paths *number*

default maximum-paths

Parameter Description

Parameter	Description
number	Number of equivalent routes in the range from 1 to 64 (vary with products).

Defaults For routers, the default value is 32. For switches, the default value varies from products.

Command Mode Global configuration mode

Usage Guide

The number of equivalent routes is configured to control the number of equivalent routes. After the number of equivalent routes is configured by running the **maximum-paths** command, the number of load-sharing channels in load-sharing mode will not exceed the number of configured static routes.

The command take effect both on IPv4 and IPv6.

You can run the **show running config** command to query the number of configured static routes.

Examples

The following example sets the number of equivalent routes to 10 and then restores the default setting.

```
maximum-paths 10
no maximum-paths 10
```

8.12 show ip redirects

Use this command to display the default gateway IP address.

show ip redirects

Use this command to display the default gateway IP address.

show ip redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the default gateway IP address. This command is supported on 2-layer devices or 3-layer devices with the **no ip routing** command executed.

Examples

The following example displays the default gateway.

```
FS# show ip redirects
Default Gateway: 192.168.195.1
```

Field	Description
Default Gateway	IP address of the default gateway.

Related Commands

Command	Description
N/A	N/A

Platform Description

8.13 show ip route

Use the commands to display the configuration of the IP routing table.

show ip route [*network* [*mask* [**longer-prefix**]] | **count** | *protocol* [*process-id*] | **weight**]]

show ip route [[**normal** | **ecmp**] [*network* [*mask*]]]

Parameter Description

Parameter	Description
network	(Optional) Displays the route information to the network.
mask	(Optional)Displays the route information to the network of this mask.
longer-prefix	(optional) Displays the routes that match the specified prefix.
count	(Optional)Displays the number of existent routes. (for the ECMP/WCMP route, displays one route)
protocol	(Optional) Displays the route information of specific protocol.
process-id	(Optional) Routing protocol process ID.
weight	(Optional) Displays the route information of non default weight.
normal	Displays normal routes and not equivalent routes or fast reroutes.
ecmp	Displays only equivalent routes.

Defaults

All routes are displayed by default.

Command Mode

Privileged EXEC mode/ Global configuration mode/Interface configuration mode/ Routing protocol configuration mode/ Route map configuration mode

Usage Guide

This command can display route information flexibly.

This command shows all routes. To show different attributes of routes, specify normal | ecmp | fast-reroute.

The following example displays the configuration of the IP routing table.

```
FS# show ip route

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, * - candidate default
Gateway of last resort is no set
S       20.0.0.0/8 is directly connected, VLAN 1
S       22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R       40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B       50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C       192.1.1.0/24 is directly connected, VLAN 1
C       192.1.1.254/32 is local host.
```

Examples

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Administrative distance/metric

```
FS# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

Field	Description
Routing Descriptor Blocks	Next hop IP address, source, update time, forwarding interface, source routing protocol and type of route information

```
FS# show ip route count
--------- route info ----------
the num of active route: 5
```

```
FS# show ip route weight
------------[distance/metric/weight]-----------
S       23.0.0.0/8 [1/0/2] via 192.1.1.20
S       172.0.0.0/16 [1/0/4] via 192.0.0.1
```

```
FS#show ip route normal

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, * - candidate default
Gateway of last resort is no set
S       20.0.0.0/8 is directly connected, VLAN 1
S       22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R       40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B       50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C       192.1.1.0/24 is directly connected, VLAN 1
C       192.1.1.254/32 is local host
```

```
FS#show ip route ecmp

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, * - candidate default
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*     0.0.0.0/0 [1/0] via 192.168.1.2
                  [1/0] via 192.168.2.2
O IA 192.168.10.0/24 [110/1] via 35.1.10.2, 00:38:26, VLAN 1
                                 [110/1] via 35.1.30.2, 00:38:26, VLAN 3
```

```
FS#show ip route fast-reroute

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, * - candidate default
Status codes: m - main entry, b - backup entry, a – active entry

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*     0.0.0.0/0 [ma] via 192.168.1.2
                  [b] via 192.168.2.2
O IA 192.168.10.0/24 [m] via 35.1.10.2, 00:38:26, VLAN 1
                          [ba]    via 35.1.30.2, 00:38:26, VLAN 3
```

```
FS# show ip route fast-reroute 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
[m] 192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
[ba]192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

8.14 show ip route summary

Use this command to display the statistical information about one routing table.

show ip route summary

Use this command to display the statistical information about all routing tables.

show ip route summary all

Parameter

Parameter	Description

Description	*N/A*	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage guideline N/A

Examples

The following example displays the statistics of the global routing table.

```
FS# show ip route summary
Codes: NORMAL – Normal route ECMP – ECMP route FRR – Fast-Reroute route

  Memory: 2000 bytes
Entries: 22,based on route prefixes
                              NORMAL ECMP FRR TOTAL
              Connected 3 0 0 3
              Static 2 1 1 4
              RIP     1 2 1 4
              OSPF 2 1 1 4

              TOTAL 11 7 4 22
```

The following example displays the statistics of all routing tables.

```
FS# show ip route summary all
Codes: NORMAL – Normal route ECMP – ECMP route FRR – Fast-Reroute route

IP routing table count:2
Total
       Memory: 4000 bytes
       Entries: 44,based on route prefixes
                              NORMAL ECMP FRR TOTAL
              Connected 6 0 0 6
              Static 4 2 2 8
              RIP     2 4 2 8
              OSPF 4 2 2 8
              ISIS 2 4 0 6
              BGP     4 2 2 8
              TOTAL 22 14 8 44

Global
       Memory: 2000 bytes
       Entries: 22,based on route prefixes
                              NORMAL ECMP FRR TOTAL
              Connected 3 0 0 3
              Static 2 1 1 4
              RIP     1 2 1 4
              OSPF 2 1 1 4
              TOTAL 11 7 4 22
```

Field	Description

NORMAL	Type of the table entries. Value:
	NORMAL: common routes (not ECMP or FRR);
	ECMP: equivalent route;
	FRR: fast reroute;
	TOTAL: total

Memory	Memory occupied by the table.
Entries	Number of entries (based on prefix, not next-hop)

Connected	Protocol type. Value:
	Connected: direct connection;
	Static: static;
	RIP: RIP;
	OSPF: OSPF;
	TOTAL: total

8.15 show ip route track-table

Use this command to display the IP route correlated Track information.

show ip route track-table

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the IP route correlated Track information.

Examples

The following example displays the IP route correlated Track information.

```
FS(config)#show ip route track-table
ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/0 track 2 state is [up]
ip route 20.0.0.0 255.0.0.0 GigabitEthernet 0/0     2 track 3 state is [down]
```

:

Field	Description
track	Track target index
state	Track target state

Related Commands

Command	Description
N/A	N/A

Platform Description

8.16 show ipv6 redirects

Use this command to display the IPv6 default gateway IP address.

show ipv6 redirects

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Examples

The following example displays the default gateway IPv6 address.

```
FS# show ipv6 redirects
Default Gateway: 10::1
```

Field	Description
Default Gateway	IPv6 address of the default gateway

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on 2-layer devices and 3-layer devices with the **no ip routing** command executed.

8.17 show ipv6 route

Use the command to display the configuration of the IPv6 routing table.

show ipv6 route [[**vrf** *vrf_name*] [*ipv6-prefix* / *prefix-length* [**longer-prefixes**] | *protocol* [*process-id*] | **weight**]]

Use the command to display the configuration of the IPv6 routing table.

show ipv6 route [[**vrf** *vrf_name*] [*ipv6-prefix* / *prefix-length* [**longer-prefixes**] | *protocol* [*process-id*] | **weight**]]

Parameter Description

Parameter	Description
vrf *vrf-name*	(Optional) Specifies a VRF.
ipv6-prefix/prefix-length	(Optional) Specifies a prefix for route’s IPv6 address.
longer-prefixes	(Optional) Displays the route with an IPv6 address prefix

	mostly matched.
protocol	((Optional) Displays the route information of specific protocol.
process-id	(Optional) Specifies a route process ID.
weight	(Optional) Displays the non-default-weight routes only.

Defaults All routes are displayed by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to display route information.

Examples

The following example displays the IPv6 routing table.

```
FS(config)# show ipv6 route

IPv6 routing table -   Default - 7 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         10::/64    via Loopback 1, directly connected
L         10::1/128    via Loopback 1, local host
S         20::/64    [20/0] via 10::4, Loopback 1C
C         FE80::/10 via Null 0, directly connected
C         FE80::/64    via Loopback 1, directly connected
L         FE80::2D0:F8FF:FE22:33AB/128    via Loopback 1, local host
```

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route

E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20::/64	Network address and mask of the destination network
[20/0]	Administrative distance/metric

Related Commands

Command	Description
ipv6 route	Configures the IPv6 static route.

Platform Description This command is not supported on 2-layer devices.

8.18 show ipv6 route summary

Use this command to display the statistics of the IPv6 routing table of a specified VRF.

show ipv6 route [**vrf** *vrf-name*] **summary**

Use this command to display statistics of all IPv6 routing tables.

show ipv6 route summary all

Parameter Description

Parameter	Description
vrf-name	(Optional) VRF name. If no VRF name is specified, statistics of the IPv6 routing table of the global VRF are displayed.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Examples

The following example displays statistics of IPv6 routing table of the global VRF.

```
FS#show ipv6 route summary
IPv6 routing table name is -    Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
```

```
Local              2
Connected           3
Static            0
PIP                0
OSPF                0
BGP                 0
------------------------
Total              5
```

The following example displays t statistics of all IPv6 routing tables.

```
FS#show ipv6 route summary
IPv6 routing table name is -    Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local              2
Connected           3
Static            0
PIP                0
OSPF                0
BGP                 0
------------------------
Total              5
```

Field	Description
Memory	The memory size occupied by the current routing table.
Entries	The entries in the current routing table (based on the entry prefix instead of the next hop entry.)
Connected	Describes the protocol type of the entry. The field can be; Connected: Connected route entry. Static: Static route entry. RIP: RIP route entry. OSPF: OSPF route entry. ISIS: ISIS route entry. BGP: BGP route entry. TOTAL: Total number of all protocol entries.
IPv6 routing table count	The number of the routing tables.
Global	The name of the current routing table. The field can be: Global : Global (The default VRF) VRF1: VRF name. TOTAL: All VRF routing table summaries.

Related Commands

Command	Description
N/A	N/A

Platform Description	This command is not supported on 2-layer devices.

Chapter 11 Security Configuration Commands

1 ACL Commands

1.1 command ID table

ID	Meaning
ID	Number of access list. Range: Standard IP ACL: 1 to 99, 1300 to 1999 Extended IP ACL: 100 to 199,2000 to 2699 Extended MAC ACL: 700 to 799 Extended expert ACL: 2700 to 2899
name	ACL name
sn	ACL SN (products can be set according to the priority)
start-sn	Start sequence number
inc-sn	Sequence number increment
deny	If matched, access is denied.
permit	If matched, access is permitted.
port	Protocol number. For IPv6, this field can be IPv6, ICMP, TCP, UDP and numbers 0 to 255. For IPv4, it can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP,AHP, ESP, PCP, PIM and IP, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as ICMP, TCP and UDP, are listed individually.
interface *idx*	Interface index
src	Packet source IP address (host address or network address)
src-wildcard	Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32.
src-ipv6-pfix	Source IPv6 network address or network type
dst-ipv6-pfix	Destination IPv6 network address or network type
pfix-len	Prefix mask length
src-ipv6-addr	Source IPv6 address
dst-ipv6-addr	Destination IPv6 address
dscp	Differential service code point, and code point value. Range: 0 to 63
flow-label	Flow label in the range 0 to 1048575
dst	Packet destination IP address (host address or network address)
dst-wildcard	Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32
fragment	Packet fragment filtering.
precedence	Packet precedence value (0 to 7)
range	The layer 4 port number range of the packet.

time-range tm-rng-name	Time range of packet filtering, named *tm-rng-name*
tos	Type of service (0 to 15)
cos	Class of service (0-7)
cos inner *cos*	COS of the packet tag
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name (0 to 255)
operator port[port]	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range) *port* indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number
src-mac-addr	Physical address of the source host
dst-mac-addr	Physical address of the destination host
VID vid	VLAN ID
VID inner vid	VID of the tag
ethernet-type	Ethernet protocol type. 0x value can be entered.
match-all *tcpf*	Match all bits of the TCP flag.
established	Match the RST or ACK bit of the TCP flag.
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface
{rule mask offset}$^{+}$	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table “+” sign indicates at least one group
log	Output the matching syslog when the packet matches the ACL rule.

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol number	35
C	Data frame length field	12	Q	IP check sum	36
D	VLAN tag field	14	R	Source IP address	38
E	DSAP (Destination Service Access Point) field	18	S	Destination IP address	42
F	SSAP (Source Service Access Point) field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54

J	IP version number	26	XY	IP header length and reserved bits	58
K	TOS field	27	Z	Resrved bits and flags bit	59
L	Length of IP packet	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

1.2 access-list

Use this command to create an access list to filter data packets. Use the **no** form of this command to remove the specified access list.

Standard IP access list (1 to 99, 1300 to 1999)

access-list *id* { **deny** | **permit** } { *source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*] [**log**]

Extended IP access list (100 to 199, 2000 to 2699)

access-list *id* { **deny** | **permit** } *protocol* { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Extended MAC access list (700 to 799)

access-list *id* { **deny** | **permit** } { **any** | *src-mac-addr* mask } { **any** | *dst-mac-addr* mask } [**cos** [*out*] [**inner** *in*]]

Extended expert access list (2700 to 2899)

access-list *id* { **deny** | **permit** } [*protocol* [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** }] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

- When you select the Ethernet-type field or cos field:

access-list *id* { **deny** | **permit** } { **cos** [*out*] [**inner** *in*] } [**VID** [*out*] [**inner** *in*]] { **s***ource source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**time-range** *time-range-name*]

- When you select the protocol field:

access-list *id* { **deny** | **permit** } *protocol* [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

- Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

access-list *id* { **deny** | **permit** } **icmp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

access-list *id* { **deny** | **permit** } **tcp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *Source* | **any** } { **any** } [**operator** port [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**operator port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)

access-list *id* { **deny** | **permit** } **udp**[**VID** [*out*] [**inner** *in*]] { *source source –wildcard* | **host** *source* | **any** } { **any** } [**operator port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**operator port** [*port*]]

[**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

Parameter Description

Parameter	Description
id	Access list number. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.
deny	If not matched, access is denied.
permit	If matched, access is permitted.
source	Specify the source IP address (host address or network address).
source-wildcard	It can be discontinuous, for example, 0.255.0.32.
protocol	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
destination	Specify the destination IP address (host address or network address).
destination-wildcard	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
precedence	Specify the packet priority.
precedence	Packet precedence value (0 to 7)
range	Layer4 port number range of the packet.
lower	Lower limit of the layer4 port number.
upper	Upper limit of the layer4 port number.
time-range	Time range of packet filtering
time-range-name	Time range name of packet filtering
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name
operator	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)
port [port]	Port number; range needs two port numbers, while other operators only need one port number.

Defaults N/A

Command Mode Global configuration mode.

Usage Guide To filter the data by using the access control list, you must first define a series of rule statements by using the access list. You can use ACLs of the appropriate types according to the security needs:

The standard IP ACL (1 to 99, 1300 to 1999) only controls the source IP addresses.

The extended IP ACL (100 to 199, 2000 to 2699) can enforce strict control over the source and destination IP addresses.

The extended MAC ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type.

The extended expert access list (2700 to 2899) is a combination of the above and can match and filter the VLAN

ID.

For the layer-3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: **precedence** *precedence* /**range** *lower upper/***time-range** *time-range-name*

The TCP Flag includes part or all of the following:

- urg
- ack
- psh
- rst
- syn
- fin

The packet precedence is as below:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The service types are as below:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The ICMP message types are as below:

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable

- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- redirect
- device-advertisement
- device-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The TCP ports are as follows. A port can be specified by port name and port number:

- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin

- kshell
- ldp
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who

- xdmcp

Configuration Examples

1. Example of the standard IP ACL

The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

```
FS (config)#access-list 1 permit 192.168.1.64 0.0.0.63
```

2. Example of the extended IP ACL

The following extended IP ACL allows the DNS messages and ICMP messages to pass:

```
FS(config)#access-list 102 permit tcp any any eq domain log
FS(config)#access-list 102 permit udp any any eq domain log
FS(config)#access-list 102 permit icmp any any echo log
FS(config)#access-list 102 permit icmp any any echo-reply
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 1/1. The configuration procedure is as below:

```
FS(config)#access-list 702 deny host 00d0f8000c0c any aarp
FS(config)# interface gigabitethernet 1/1
FS(config-if)# mac access-group 702 in
```

4. Example of the extended expert ACL

The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
FS(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
FS(config)# access-list 2702 permit any any any any
FS(config)# show access-lists
expert access-list extended 2702
10 deny tcp    host    192.168.12.3 mac 00d0.f800.0044 any any
10 permit any any any any
```

Related Commands

Command	Description
show access-lists	Show all the ACLs.
mac access-group	Apply the extended MAC ACL on the interface.

Platform Description

N/A

1.3 access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

access-list *id* **list-remark** *text*

no access-list *id* **list-remark**

Parameter Description

Parameter	Description

id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
text	Comment that describes the access list.

Defaults The access lists have no remarks by default.

Command Mode Global configuration mode

Usage Guide You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.

Configuration Examples The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL100.

```
FS(config)# ip access-list extended 100
FS(config)# access-list 100 list-remark this acl is to filter the host 192.168.4.12
```

Related Commands

Command	Description
show access- lists	Displays all access lists, including the remarks for the access lists.
show access-lists *id*	Displays the access list of a specified number, including the remarks for the access list.
show access-lists *name*	Displays the access list of a specified name, including the remarks for the access list.

Platform Description

1.4 access-list remark

Use this command to write a helpful comment (remark) for an entry in a numbered access list. Use the **no** form of this command to remove the remark.

access-list *id* **remark** *text*

no access-list *id* **remark** *text*

Parameter Description

Parameter	Description
id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199. 2000 to 2699. Extended MAC ACL: 700 to 799.

	Extended Expert ACL: 2700 to 2899.
text	Comment that describes the access list entry.

Defaults The access list entries have no remarks by default.

Command Mode Global configuration mode

Usage Guide You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.

Configuration Examples The following example writes a comment for an entry in ACL102.

```
FS(config)# access-list 102 remark deny-host-10.1.1.1
```

Related Commands

Command	Description
show access-lists	Displays all access lists, including the remarks for the access list entries.
show access-lists *id*	Displays the access list of a specified number, including the remarks for the access list entry.
show access-lists *name*	Displays the access list of a specified name, including the remarks for the access list entry.

Platform Description

1.5 clear access-list counters

Use this command to clear counters of packets matching the deny entries in ACLs.

clear access-list counters [*id* | *name*]

Parameter Description

Parameter	Description
id	Access list number ● Standard IP ACL: 1-99, 1300-1999 ● Extended IP ACL:100-199, 2000-2699 ● Extended MAC ACL: 700-799 ● Extended expert ACL: 2700-2899
name	Access list name

Defaults

Command Mode Privileged EXEC mode

Usage Guide

This command is used to clear the counters of packets matching the deny entries in ACLs.

Configuration Examples

The following example clears the packet matching counter of ACL No. 1:

Before configuration:

```
FS #show access-lists
ip access-list standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches)
    (10 packets filtered)
```

After configuration:

```
FS# end
FS# clear access-list counters
FS# show access-lists
ip access-list standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches)
```

Related Commands

Command	Description
expert access-list	Defines an expert ACL.
deny	Defines a deny ACL entry.
permit	Defines a permits ACL entry.

Platform Description

N/A

1.6 clear counters access-list

Use this command to clear counters of packets matching ACLs.

clear counters access-list [*id* | *name*]

Parameter Description

Parameter	Description
id	Access list number. Configurable range: ● Standard IP ACL: 1-99, 1300-1999 ● Extended IP ACL:100-199, 2000-2699 ● Extended MAC ACL: 700-799 ● Extended expert ACL: 2700-2899
name	Access list name

Defaults

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the counters of packets matching the specified or all ACLs.

Configuration Examples

The following example clears the packet matching counter of ACL No. 2700:

```
FS #show access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any    (88 matches)
    20 deny tcp any any eq login any any (33455 matches)
    30 permit tcp any any host 192.168.6.9 any (10 matches)

FS# clear counters access-list 2700
FS #show access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
    20 deny tcp any any eq login any any
    30 permit tcp any any host 192.168.6.9 any
```

Related Commands

Command	Description
expert access-list	Defines an expert ACL.
deny	Defines a deny ACL entry.
permit	Defines a permits ACL entry.

Platform Description

N/A

1.7 deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

1. Standard IP ACL

Use this command to add a standard IP ACL.

Use the **no** form of this command to remove a standard IP ACL.

[*sn*] **deny** {*source source-wildcard* | **host** *source* | **any| interface** *idx* }[**time-range** *tm-range-name*] [**log**]

no { *sn* | { **deny** { *source source-wildcard* | **host** *source* | **any** } [**time-range** *tm-range-name*] [**log**] } }

Extended IP ACL

Use this command to add an extended IP ACL.

Use the **no** form of this command to remove an extended IP ACL.

[*sn*] **deny protocol source** *source-wildcard* **destination** *destination-wildcard* [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

no [*sn*] **deny protocol source** *source-wildcard* **destination** *destination-wildcard* [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

Extended IP ACLs of some important protocols:

- Internet Control Message Prot (ICMP)

[*sn*] **deny icmp** { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

- Transmission Control Protocol (TCP)

[*sn*] **deny tcp** { *source source-wildcard* | **host** *Source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

- User Datagram Protocol (UDP)

[*sn*] **deny udp** { *source source –wildcard* | **host** *source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended MAC ACL

Use this command to add an extended MAC ACL.

Use the **no** form of this command to remove an extended MAC ACL.

[*sn*] **deny** { **any** } { **any** } [**cos** [*out*] [**inner** *in*]]

no { *sn* | {**deny** { **any** } { **any** } [**cos** [*out*] [**inner** *in*]] } }

Extended expert ACL

Use this command to add an extended expert ACL.

Use the **no** form of this command to remove an extended expert ACL.

[*sn*] **deny**[*protocol* | [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any**}{ **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

no { *sn* | { **deny** [*protocol* | [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] } }

- When you select the ethernet-type field or cos field:

[*sn*] **deny** [**cos** [*out*] [**inner** *in*]] } [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**time-range** *time-range-name*]

- When you select the protocol field:

[*sn*] **deny protocol** [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destinationdestination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*]

[**time-range** *time-range-name*]

- Extended expert ACLs of some important protocols

Internet Control Message Protocol (ICMP)

[*sn*] **deny icmp** [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **deny tcp** [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *Source* | **any** } { **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)

[*sn*] **deny udp** [[**VID** [*out*] [**inner** *in*]]] { *source source –wildcard* | **host** *source* | **any** } { **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **deny arp** { **vid** *vlan-id* } [*source-mac-address source-wildcard* **| any**] [**host** *destination –mac-address* | **any**] { *sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any** } { *sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any** } { *target-ip target-ip–wildcard* | **host** *target-ip* | **any** }

Parameter Description

Parameter	Description
sn	ACL entry sequence number
prefix-length	Prefix mask length
flow-label	Flow label
flow-label	Flow label value, within the range of 0 to 1048575.
protocol	For the IPv6, the field can be ipv6 | icmp | tcp | udp and number in the range 0 to 255
time-range	Time range of the packet filtering
time-range-name	Time range name of the packet filtering

Defaults No entry

Command mode ACL configuration mode.

Usage Guide Use this command to configure the filtering entry of ACLs in ACL configuration mode.

Configuration Examples The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
FS(config)#expert access-list extended 2702
FS(config-exp-nacl)#deny tcp   host
192.168.4.12 host 0013.0049.8272 any any
FS(config-exp-nacl)#permit any any any any
FS(config-exp-nacl)#show access-lists
expert access-list extended 2702
10 deny tcp   host   192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
FS(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)# ip access-list extended ip-ext-acl
FS(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
FS(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
FS(config-ext-nacl)#exit
FS(config)#interface gigabitethernet 1/1
FS(config-if)#ip access-group ip-ext-acl in
FS(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)#mac access-list extended mac1
FS(config-mac-nacl)#deny host 0013.0049.8272 any aarp
FS(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
FS(config-mac-nacl)#exit
FS(config)# interface gigabitethernet 1/1
FS(config-if)# mac access-group mac1 in
```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)#ip access-list standard 34
FS(config-ext-nacl)# deny host 192.168.4.12
FS(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
FS(config-ext-nacl)#exit
FS(config)# interface gigabitethernet 1/1
FS(config-if)# ip access-group 34 in
```

Related Commands

Command	Description
show access-lists	Displays all ACLs.
ipv6 traffic-filter	Applies the extended IPv6 ACL on the interface.
ip access-group	Applies the IP ACL on the interface.
mac access-group	Applies the extended MAC ACL on the interface.
ip access-list	Defines an IP ACL.
mac access-list	Defines an extended MAC ACL.
expert access-list	Defines an extended expert ACL.
ipv6 access-list	Defines an extended IPv6 ACL.
permit	Permits the access.

Platform Description

N/A

1.8 ip access-group

Use this command to apply a specific access list globally or to an interface. Use the **no** form of this command to remove the access list from the interface.

ip access-group { *id* | *name* } { **in** | **out** }

no ip access-group { *id* | *name* } { **in** | **out** }

Parameter Description

Parameter	Description
id	IP access list or extended IP access list number: 1 to 199, 1300 to 2699
name	Name of the IP ACL
in	Filters the incoming packets of the interface.
out	Filters the outgoing packets of the interface.

Defaults

No access list is applied globally or on the interface by default.

Command mode

Global, interface configuration mode.

Usage Guide

Use this command to control access to a specified interface globally.

Configuration Examples

The following example applies the ACL 120 on interface fastEthernet0/0 to filter the incoming packets:

```
FS(config)# interface fastEthernet 0/0
FS(config-if)# ip access-group 120 in
```

Related Commands

Command	Description
access-list	Defines an ACL.

show access-lists	Displays all ACLs.

Platform Description

N/A

1.9 ip access-list

Use this command to create a standard IP access list or extended IP access list. Use the **no** form of the command to remove the access list.

ip access-list {**extended** | **standard**} {*id* | *name*}

no ip access-list {**extended** | **standard**} {*id* | *name*}

Parameter Description

Parameter	Description
id	Access list number: Standard: 1 to 99, 1300 to 1999; Extended: 100 to 199, 2000 to 2699.
name	Name of the access list

Defaults

N/A

Command mode

Global configuration mode

Usage Guide

Configure a standard access list if you need to filter on source address only. If you want to filter on anything other than source address, you need to create an extended access list.

Refer to **deny** or **permit** in the two modes. Use the **show access-lists** command to display the ACL configurations**.**

Configuration Examples

The following example creates a standard access list named std-acl.

```
FS(config)# ip access-list standard std-acl
FS(config-std-nacl)# show access-lists
ip access-list standard std-acl
FS(config-std-nacl)#
```

The following example creates an extended ACL numbered 123:

```
FS(config)# ip access-list extended 123
FS(config-ext-nacl)# show access-lists
ip access-list extended 123
```

Related Commands

Command	Description
show access-lists	Displays all ACLs.

Platform Description

N/A

1.10 ip access-list counter

Use this command to enable the counter of packets matching the standard or extended IP access list. Use the **no** form of this command to disable the counter.

ip access-list counter { *id* | *name* }

no ip access-list counter { *id* | *name* }

Parameter Description

Parameter	Description
id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the IP access list.

Defaults

The counter of packets matching the standard or extended IP access list is disabled by default.

Command mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the counter of packets matching the standard access list:

```
FS(config)# ip access-list counter std-acl
FS(config-std-nacl)# show access-lists
ip access-list standard std-acl
  10 permit 195.168.6.0 0.0.0.255 (999 matches)
  20 deny host 5.5.5.5 time-range tm (2000 matches)
```

The following example disables the counter of packets matching the standard access list:

```
FS(config)#no ip access-list counter std-acl
FS(config-std-nacl)# show access-lists
ip access-list standard std-acl
  10 permit 195.168.6.0 0.0.0.255
  20 deny host 5.5.5.5 time-range tm
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description

N/A

1.11 ip access-list log-update interval

Use this command to configure the interval at which the IPv4 access list log is updated. Use the **no** form of this command to restore the default interval.

ip access-list log-update interval *time*

no ip access-list log-update interval

Parameter Description

Parameter	Description
time	For the access rule with the **log** option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specified flow is output every 5 minutes. 0 indicates that no ACL logging is output.

Defaults The default interval at which the IPv4 access list log is updated is 5 minutes.

Command mode Global configuration mode

Usage Guide Use this command to configure the interval at which the IPv4 access list log is updated.

Configuration Examples The following example configures the interval for the IPv4 access list log update to 10 minutes:

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# ip access-list log-update interval 10
```

Related Commands

Command	Description
ip access-list	Defines an IPv4 access list.
deny	Defines the **deny** access entries.
permit	Defines the **permit** access entries.
show running	Displays running configurations of the device.

Platform Description N/A

1.12 ip access-list resequence

Use this command to resequence a standard or extended IP access list. Use the **no** form of this command to restore the default order of access entries.

ip access-list resequence { *id* | *name* } *start-sn inc-sn*

no ip access-list resequence { *id* | *name* }

Parameter Description

Parameter	Description

id	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
name	Name of the standard or extended IP access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use this command to change the order of the access entries.

Configuration Examples

The following example resequences entries of ACL1:

Before the configuration:

```
FS# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
```

After the configuration:

```
FS# config
FS(config)# ip access-list resequence 1 21 43
FS(config)# exit
FS# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description

N/A

1.13 ipv6 access-list

Use this command to create an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the **no** form of this command to remove the access list.

ipv6 access-list *name*

no ipv6 access-list *name*

Parameter Description

Parameter	Description
name	Name of the IPv6 access list.

Defaults

N/A

Command mode

Global configuration mode

Usage Guide

To filter the IPv6 packets through the access list, you need to define an IPv6 access list by using the **ipv6 access-list** command.

Configuration Examples

The following example creates an IPv6 access list named v6-acl:

```
FS(config)# ipv6 access-list v6-acl
FS(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
FS(config-ipv6-nacl)#
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description

N/A

1.14 ipv6 access-list counter

Use this command to enable the counter of packets matching the IPv6 access list. Use the **no** form of this command to disable the counter.

ipv6 access-list counter *name*

no ipv6 access-list counter *name*

Parameter Description

Parameter	Description
name	Name of the IPv6 access list.

Defaults

-

Command mode

Global configuration mode

Usage Guide

Use this command to enable the counter of packets matching the IPv6 access list to monitor the IPv6 packets matching and filtering.

Configuration Examples

The following example enables the counter of packets matching the IPv6 access list named v6-acl:

```
FS(config)# ipv6 access-list v6-acl
FS(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
  10 permit icmp any any (7 matches)
  20 deny tcp any any (7 matches)
```

The following example disables the counter of packets matching the IPv6 access list named v6-acl:

```
FS(config)#no ipv6 access-list v6-acl counter
FS(config-ipv6-nacl)# show access-lists
ipv6 access-list acl-v6
  10 permit icmp any any
20 deny tcp any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists.

Platform Description

N/A

1.15 ipv6 access-list log-update interval

Use this command to configure the interval at which the IPv6 access list log is updated. Use the **no** form of this command to restore the default interval.

ipv6 access-list log-update interval *time*

no ipv6 access-list log-update interval

Parameter Description

Parameter	Description
time	For the access rule with the **logging** option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specific flow is output every 5 minutes. 0 indicates that no ACL logging is output.

Defaults

N/A

Command mode

Global configuration mode

Usage Guide

Use this command to configure the interval at which the IPv6 access list log is updated.

Configuration Examples

The following example configures the interval for the IPv6 access list log update to 10 minutes:

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# ipv6 access-list log-update interval 9
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list.
deny	Defines the **deny** access entries.
permit	Defines the **permit** access entries.
show running	Displays the running configurations of the device.

Platform Description

N/A

1.16 ipv6 access-list resequence

Use this command to resequence an IPv6 access list. Use the **no** form of this command to restore the default order of access entries.

ipv6 access-list resequence *name start-sn inc-sn*

no ipv6 access-list resequence *name*

Parameter Description

Parameter	Description
name	Name of the IPv6 access list
start-sn	Start sequence number. Range: 1 to 2147483647
inc-sn	Increment of the sequence number. Range: 1 to 2147483647

Defaults

start-sn: 10

inc-sn: 10

Command mode

Global configuration mode

Usage Guide

Use this command to change the order of the access entries.

Configuration Examples

The following example resequences entries of IPv6 access list “v6-acl”:

Before the configuration:

```
FS# show access-lists
ipv6 access-list v6-acl
  10 permit ipv6 any any
  20 deny ipv6 any any
```

After the configuration:

```
FS# config
FS(config)# ipv6 access-list resequence v6-acl 21 43
FS(config)# exit
FS# show access-lists
ipv6 access-list v6-acl
  21 permit ipv6 any any
  64 deny ipv6 any any
```

Related Commands

Command	Description
show access-lists	Displays all access lists..

Platform Description

N/A

1.17 ipv6 traffic-filter

Use this command to apply an IPV6 access list globally or on the specified interface/VXLAN. Use the **no** form of the command to remove the IPv6 access list from the interface/VXLAN.

ipv6 traffic-filter *name* { **in** | **out** }

no ipv6 traffic-filter *name* { **in** | **out** }

Parameter Description

Parameter	Description
name	Name of IPv6 access list
in	Specifies filtering on inbound packets
out	Specifies filtering on outbound packets

Defaults

N/A

Command mode

Global/Interface/VXLAN configuration mode.

Usage Guide

Use this command to apply the IPv6 access list globally or on a specified interface/VXLAN to filter the inbound or outbound packets.

Configuration Examples

The following example applies the IPv6 access list named **v6-acl** to interface GigabitEthernet 0/1:

```
FS(config)# interface GigaEthernet 0/1
FS(config-if)# ipv6 traffic-filter v6-acl in
```

The following example applies the IPv6 access list named **v6-acl** to VXLAN1:

```
FS(config)#vxlan 1
FS(config-vxlan)#ipv6 traffic-filter v6-acl in
```

Related Commands

Command	Description

show access-group	Displays ACL configurations on the interface.

Platform Description N/A

1.18 list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

list-remark *text*

no list-remark

Parameter Description

Parameter	Description
text	Comment that describes the access list.

Defaults The access lists have no remarks by default.

Command mode ACL configuration mode

Usage Guide You can use this command to write a helpful comment for a specified access list.

Configuration Examples The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL102.

```
FS(config)# ip access-list extended 102
FS(config-ext-nacl)# list-remark this acl is to filter the host 192.168.4.12
FS(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
1000 hits
this acl is to filter the host 192.168.4.12
FS(config-ext-nacl)#
```

Related Commands

Command	Description
show access-lists	Displays all access lists.
ip access-list	Defines an IPv4 access list.
access-list list remark	Adds a helpful comment for an access list in global configuration mode.

Platform Description N/A

1.19 permit

One or multiple **permit** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

1. Standard IP ACL

Use this command to add a standard IP ACL.

Use the **no** form of this command to remove a standard IP ACL.

[*sn*] **permit** {*source source-wildcard* | **host** *source* | **any | interface** *idx* } [**time-range** *tm-range-name*] [**log**]

no { *sn* | { **permit** { *source source-wildcard* | **host** *source* | **any** } [**time-range** *tm-range-name*] [**log**] } }

2. Extended IP ACL

Use this command to add an extended IP ACL.

Use the **no** form of this command to remove an extended IP ACL.

[*sn*] **permit protocol** *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

no { *sn* | { **permit protocol** *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**] } }

Extended IP ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** { *source source-wildcard* | **host** *Source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)

[*sn*] **permit udp** { *source source –wildcard* | **host** *source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [**operator port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

3. Extended MAC ACL

Use this command to add an extended MAC ACL.

Use the **no** form of this command to remove an extended MAC ACL.

[*sn*] **permit** { **any** | *source-mac-address mask*} { **any** | *destination -mac-address mask* } [**cos** [*out*] [**inner** *in*]]

no { *sn* | { **permit** { **any** | *source-mac-address mask*} { **any** | *destination -mac-address mask* } [**cos** [*out*] [**inner** *in*]] } }

4. Extended expert ACL

Use this command to add an extended expert ACL.

Use the **no** form of this command to remove an extended expert ACL.

[*sn*] **permit** [**protocol** | [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

no { *sn* | { **permit** [**protocol** | [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] } }

When you select the cos field:

[*sn*] **permit** { **cos** [*out*] [**inner** *in*] } [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**time-range** *time-range-name*]

When you select the protocol field:

[*sn*] **permit protocol** [**VID** [*out*] [**inner** *in*] { *source source-wildcard* | **host** *Source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

[*sn*] **permit icmp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **permit tcp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *Source* | **any** } { **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)

[*sn*] **permit udp** [**VID** [*out*] [**inner** *in*]] { *source source –wildcard* | **host** *source* | **any** } { **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **permit arp** { **vid** *vlan-id* } [**any**] [**host** *destination –mac-address* | **any**] { *sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any** } { *sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any** } { *target-ip target-ip–wildcard* | **host** *target-ip* | **any** }

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults N/A

Command mode

ACL configuration mode.

Usage Guide

Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.

Configuration Examples

The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
FS(config)#expert access-list extended exp-acl
FS(config-exp-nacl)#permit tcp   host   192.168.4.12 host 0013.0049.8272 any any
FS(config-exp-nacl)#deny any any any any
FS(config-exp-nacl)#show access-lists
expert access-list extended exp-acl
10 permit tcp   host   192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
FS(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)# ip access-list extended 102
FS(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
FS(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
FS(config-ext-nacl)#exit
FS(config)#interface gigabitethernet 1/1
FS(config-if)#ip access-group 102 in
FS(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)#mac access-list extended 702
FS(config-mac-nacl)#permit host 0013.0049.8272 any aarp
FS(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
FS(config-mac-nacl)#exit
FS(config)#interface gigabitethernet 1/1
FS(config-if)#mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)#ip access-list standard std-acl
FS(config-std-nacl)#permit host 192.168.4.12
FS(config-std-nacl)#show access-lists
ip access-list standard std-acl
   10 permit host 192.168.4.12
FS(config-std-nacl)#exit
FS(config)# interface gigabitethernet 1/1
FS(config-if)# ip access-group std-acl in
```

This example shows how to use the advanced expert ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)# expert access-list advanced adv-acl
FS(config-exp-dacl)# permit a0c8040c ffffffff 38
FS(config-exp-dacl)# show access-lists
expert access-list advanced adv-acl
10 permit a0c8040c ffffffff 38
FS(config-exp-dacl)# exit
FS(config)# interface gigabitethernet 1/1
FS(config-if)# expert access-group adv-acl in
```

Related Commands

Command	Description
show access-lists	Displays all access lists.
ipv6 traffic-filter	Applies the extended IPv6 access list to the interface.
ip access-group	Applies the IP access list to the interface.
mac access-group	Applies the extended MAC access list to the interface.
ip access-list	Defines an IP access list.
mac access-list	Defines an extended MAC access list.
expert access-list	Define an extended expert access list.
ipv6 access-list	Defines an extended IPv6 access list.
deny	Defines the **deny** access entry.

Platform Description

N/A

1.20 remark

Use this command to write a helpful comment (remark) for an entry in the access list. Use the **no** form of this command to remove the remark.

remark *text*

no remark

Parameter Description

Parameter	Description

text	Comment that describes the access entry.

Defaults The access entries have no remarks.

Command mode ACL configuration mode.

Usage Guide Use this command to write a helpful comment for an access entry.

Up to 100 characters are allowed in the remark.

Two identical access entry remarks in one access list is not allowed.

Removing an access entry may delete the remark for it as well.

Configuration Examples The following example writes remarks for the entry in extended IP access list 102.

```
FS(config)# ip access-list extended 102
FS(config-ext-nacl)# remark first_remark
FS(config-ext-nacl)# permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
FS(config-ext-nacl)# remark second_remark
FS(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
FS(config-ext-nacl)# end
FS#
```

Related Commands

Command	Description
show access-lists	Displays all access lists.
ip access-list	Defines an IP access list.

Platform Description N/A

1.21 show access-group

Use this command to display the access list applied to the interface.

show access-group [**interface** *interface-name*] | [**wlan** wlan-id]

Parameter Description

Parameter	Description
interface *Interface-name*	Interface name
wlan *wlan-id*	WLAN ID

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide

Use this command to display the access list configuration on the specified interface. If no interface is specified, access list configuration on all interfaces is displayed.

Configuration Examples

The following example displays interfaces where the access list is applied and the directions of these lists.

```
FS# show access-group
ip access-list standard ipstd3 in
Applied On interface GigabitEthernet 0/1.
ip access-list standard ipstd4 out
Applied On interface GigabitEthernet 0/2.
ip access-list extended 101 in
Applied On interface GigabitEthernet 0/3.
ip access-list extended 102 in
Applied On interface GigabitEthernet 0/8.
```

The following example displays whether any ACL is applied to the interface GigabitEthernet 0/3 and the directions of the ACL.

```
FS# show access-group interface GigabitEthernet 0/3
ip access-list extended 101
Applied On interface GigabitEthernet 0/3 in.
```

Related Commands

Command	Description
ip access-group	Applies the IP access list to the interface.
mac access-group	Applies the MAC access list to the interface.
expert access-group	Applies the expert access list to the interface.
ipv6 traffic-filter	Applies the IPv6 access list to the interface.

Platform Description

N/A

1.22 show access-lists

Use this command to display all access lists or the specified access list.

show access-lists [*id* | *name*] [**summary**]

Parameter Description

Parameter	Description
id	Access list number
name	Name of the IP access list
summary	Access list summary

Defaults

N/A

Command

Global configuration mode

mode

Usage Guide Use this command to display the specified access list. If no access list number or name is specified, all the access lists are displayed.

Configuration Examples

```
FS# show access-lists n_acl
ip access-list standard n_acl
ip access-list extended 101
permit icmp host 192.168.1.1 any log (1080 matches)
    permit tcp host 1.1.1.1 any established
    deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
petmit ipv6 ::192.168.4.12 any (100 matches)
deny any any (9 matches)
```

Related Commands

Command	Description
ip access-list	Defines an IP access list.
mac access-list	Defines an extended MAC access list.
expert access-list	Defines an extended expert access list.
ipv6 access-list	Defines an extended IPv6 access list.

Platform Description N/A

1.23 show ip access-group

Use this command to display the standard and extended IP access lists on the interface.

show ip access-group [**interface** *interface*] | [**wlan** *wlan-id*]

Parameter Description

Parameter	Description
interface	Interface name
wlan-id	WLAN ID

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Use this command to display the standard and extended IP access lists configured on the interface. If no interface is specified, the standard and extended IP access lists on all interfaces are displayed.

Configuration Examples

```
FS# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

Related Commands

Command	Description
ip access-list	Defines an IP access list.

Platform Description

N/A

1.24 show ipv6 traffic-filter

Use this command to display the IPv6 access list on the interface.

show ipv6 traffic-filter [**interface** *interface-name*]

Parameter Description

Parameter	Description
Interface-name	Interface name

Defaults

-

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the IPv6 access list configured on the interface. If no interface is specified, the IPv6 access lists on all interfaces are displayed.

Configuration Examples

```
FS# show ipv6 traffic-filter interface gigabitethernet 0/4
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/4.
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list.

Platform Description

N/A

2 RPL Commands

2.1 reverse-path

Enable the RPL module.

reverse-path

Disable the RPL module.

no reverse-path

Restore default settings.

default reverse-path

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, the RPL module is disabled.

Command Mode Interface configuration mode

Default Level 14

Usage Guide Run the **reverse-path** command to enable the RPL module on an interface so that it can return new data flows along the same path where the data flows are sent. Use the **no** form of this command to disable the RPL module. The command is only applicable to new data flows.

Configuration Example 1. Enable the RPL module.

```
FS(config-if-GigabitEthernet 0/1)#reverse-path
```

2. Disable the RPL module.

```
FS(config-if-GigabitEthernet 0/1)#no reverse-path
```

Verification Run the **show running-config** command to check whether the RPL module is enabled.

3 RNFP Commands

3.1 acpp

Configure ACPP.

acpp bw-rate *rate* **bw-burst-rate** *burst-rate* [**log**]

Disable ACPP.

no acpp

Restore the default configuration.

default acpp

Parameter Description

Parameter	Description
rate	Indicates rate limit. The unit is pps. The value ranges from 1 to 600.
burst-rate	Indicates burst rate limit. The unit is pps. The value ranges from 1 to 600.
log	Prints logs by the console.

Defaults

ACPP is disabled.

Command Mode

control-plane configuration mode. The function can be configured on the three sub-interfaces.

Default Level

14

Usage Guide

To configure ACPP, run the **acpp** command in control-plane configuration mode.

Configuration Example

1. Set the rate of data traffic to 200 pps and allowable burst rate to 300 pps.

```
FS(config)# control-plane data
FS(config-cp)# acpp bw-rate 200 bw-burst-rate 300
```

Verification

1. Run the **show ef-rnfp acpp** { **data** | **manage** | **protocol** } command to check whether ACPP is enabled as well as the packet loss status.

Prompt

1. If no ACPP policy is configured on a sub-interface, when the **no acpp** or **default acpp** operation is performed, a prompt will be displayed, indicating that the delete operation failed.

```
FS(config)# control-plane manage
FS(config-cp)# no acpp
EF-RNFP:    delete acpp rule failed
FS(config-cp)# default acpp
```

```
EF-RNFP:    delete acpp rule failed
```

3.2 anti-arp-spoof

Configure ARP attack detection.

anti-arp-spoof [**scan** *arp-num*]

Disable ARP attack detection.

no anti-arp-spoof [**scan** *arp-num*]

Restore the default configuration.

default anti-arp-spoof [**scan** *arp-num*]

Parameter Description

Parameter	Description
anti-arp-spoof	Enables ARP attack detection.
arp-num	Configures the ARP scanning value.

Defaults

The function is disabled.

Command Mode

control-plane configuration mode

Default Level

14

Usage Guide

If ARP anti-attack is enabled and this command is configured, 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 request packets 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 packet is different from the existing MAC address.

Configuration Example

1. Enable ARP attack detection and set the ARP scanning threshold to 30.

```
FS(config)# control-plane
FS(config-cp)# anti-arp-spoof
FS(config-cp)# anti-arp-spoof 30
```

Verification

1. Run the **show ef-rnfp anti-arp-spoof** command to check whether the function is enabled.

Run the **show arp-suspect** command to display the ARP spoofing suspect list.

Platform Description

3.3 arp-car

Configure ARP-CAR.

arp-car *packet_rate_per_group* [**log**]

Disable ARP-CAR.

no arp-car

Restore the default configuration.

default arp-car

Parameter Description

Parameter	**Description**
packet_rate_per_group	Indicates the ARP-CAR rate limit value. The unit is pps. The value ranges from 1 to 20.
log	Prints logs by the console.

Defaults ARP-CAR is disabled.

Command Mode control-plane configuration mode. The function can be configured only on the manage sub-interface.

Default Level 14

Usage Guide To configure Glean-CAR to rate the limit of received ARP packets, run the **arp-car** command in control-plane configuration mode.

Configuration Example 1. Limit the rate to 10 pps on the manage sub-interface for ARP traffic initiated by users (sources) who are in the same group according to the hash algorithm.

```
FS(config)# control-plane manage
FS(config-cp)# arp-car 10
```

Verification 1. Run the **show ef-rnfp arp-car** command to check whether ARP-CAR is enabled as well as the packet loss status.

Prompt 1. If no Glean-CAR policy is configured on the data sub-interface, when the **no** or **default** operation is performed, a prompt will be displayed, indicating that the delete operation failed.

```
FS(config)# control-plane data
FS(config-cp)# no glean-car
EF-RNFP:    delete glean-car rule failed
FS(config-cp)# default glean-car
EF-RNFP:    delete glean-car rule failed
```

3.4 attack threshold

Configure the attack confirmation threshold.

attack threshold *drop-num*

Delete the attack confirmation threshold.

no attack threshold

Restore the default configuration.

default attack threshold

Parameter Description

Parameter	Description
drop-num	Indicates the packet loss rate threshold for judging whether an attack occurs. The value ranges from 100 pps to 100,000 pps.

Defaults

attack threshold 500

Command Mode

control-plane configuration mode

Default Level

14

Usage Guide

When the packet loss per second reaches this value, the device considers that attacks occur on the network. If the network environment is not good, set this threshold to a larger value.

Configuration Example

1. Set the attack judgment threshold to 1000.

```
FS(config)# control-plane
FS(config-cp)# attack threshold 1000
```

Verification

1. Run the **show run** command to display the attack threshold.

3.5 clear attack-info history

Clear historical attack records.

clear attack-info history

Parameter Description

Parameter	Description
history	Indicates historical attack records.

Defaults

N/A

Command

Privileged EXEC mode

Mode

Default Level 14

Configuration Example

1. Clear the history.

```
FS# clear attack-info history
```

Verification

1. Run the **show attack-info history** command to display the attack history.

Prompt

The following prompt is displayed if the history is cleared successfully.

```
FS# clear attack-info history
The history attack record has been cleared!
```

3.6 control-plane

Enter the control-plane configuration mode.

control-plane [**protocol** | **manage** | **data**]

Parameter Description

Parameter	Description
protocol	Enters the protocol sub-interface.
manage	Enters the manage sub-interface.
data	Enters the data sub-interface.
N/A	Configure local anti-attack parameters globally.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide Different rules need to be configured on different sub-interfaces. Therefore, you need to enter a specific sub-interface to configure different rate limit rules.

Configuration Example

1. Enter the protocol sub-interface.

```
FS(config)# control-plane protocol
FS(config-cp)#
```

3.7 ef-rnfp enable

Enable local anti-attack.

ef-rnfp enable

Disable local anti-attack.

no ef-rnfp enable

Restore the default configuration.

default ef-rnfp enable

Parameter Description

Parameter	Description
enable	Indicates the function switch.

Defaults The function is disabled.

Command Mode control-plane configuration mode

Default Level 14

Usage Guide To enable device anti-attack, run the **ef-rnfp enable** command. The anti-attack function is enabled only after this command is run.

If no policy is configured on all sub-interfaces, the system automatically generates the default rate limit policy.

Configuration Example 1. Enable the anti-attack function.

```
FS(config)# control-plane
FS(config-cp)# ef-rnfp enable
```

Verification 1. Run the **show run** command to check whether the local anti-attack is enabled.

3.8 glean-car

Configure Glean-CAR.

glean-car *packet_rate_per_group* [**log**]

Disable Glean-CAR.

no glean-car

Restore the default configuration.

default glean-car

Parameter Description

Parameter	Description
packet_rate_per_group	Indicates the Glean-CAR rate limit value. The unit is pps.

log	Prints logs by the console.

Defaults

Glean-CAR is disabled.

Command Mode

control-plane configuration mode. The function can be configured only on the data sub-interface.

Default Level

14

Usage Guide

To configure Glean-CAR to rate the limit of traffic that is matched to the directly connected route after routing but whose destination IP address is not resolved, run the **glean-car** command in control-plane configuration mode.

Configuration Example

1. Set the rate limit to 10 pps 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.

```
FS(config)# control-plane data
FS(config-cp)# glean-car 10
```

Verification

Run the **show ef-rnfp arp-car** command to check whether Glean-CAR is enabled as well as the packet loss status.

Prompt

1. If no Glean-CAR policy is configured on the data sub-interface, when the **no** or **default** operation is performed, a prompt will be displayed, indicating the delete operation failed.

```
FS(config)# control-plane data
FS(config-cp)# no glean-car
EF-RNFP:    delete glean-car rule failed
FS(config-cp)# default glean-car
EF-RNFP:    delete glean-car rule failed
```

3.9 management-interface

Configure Management Plane Protection (MPP).

management-interface *interface* **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** } [**log**]

Disable MPP on an interface.

no management-interface *interface*

Restore the default configuration.

default management-interface

Parameter Description

Parameter	Description
interface	Specifies the management interface.
ftp	Specifies the management interfaces that accept FTP.

http	Specifies the management interfaces that accept HTTP.
ssh	Specifies the management interfaces that accept SSH.
snmp	Specifies the management interfaces that accept SNMP.
telnet	Specifies the management interfaces that accept Telnet.
tftp	Specifies the management interfaces that accept TFTP.
log	Prints logs by the console.

Defaults The MPP function is disabled.

Command Mode control-plane configuration mode. The function can be configured only on the manage sub-interface.

Default Level 14

Usage Guide MPP allows administrators to specify one or multiple interfaces as the inband management interfaces (receiving management packets and forwarding normal services). After MPP is enabled, only specified inband management interfaces are allowed to receive management packets of a specified protocol. To configure MPP, run the **management-interface** command in control-plane configuration mode.

Configuration Example 1. Specify Port Gi0/0 as the inband management interface, and allow only the interface to receive the Telnet and SNMP protocol packets.

```
FS(config)# control-plane manage
FS(config-cp)# management-interface gi 0/0 allow snmp telnet
```

Verification 1. Run the **show ef-rnfp mpp** command to check whether MPP is enabled or disabled as well as the packet loss status.

Prompt 1. If no MPP policy is configured on the manage sub-interface, when the **no** operation is performed, a prompt will be displayed, indicating that the delete operation failed.

```
FS(config)# control-plane manage
FS(config-cp)# no management-interface gi 0/1
EF-RNFP:    delete mpp rule failed
```

3.10 port-filter

Configure Port-Filter.

port-filter [**log**]

Disable Port-Filter.

no port-filter

Restore the default configuration.

default port-filter

Parameter Description

Parameter	Description
port-filter	Enable Port-Filter.
log	Prints logs by the console.

Defaults

Port-Filter is disabled.

Command Mode

control-plane configuration mode. The function can be configured only on the manage sub-interface.

Default Level

14

Usage Guide

The Port-Filter function can filter out local illegitimate transport-layer packets, of which the destination port is not enabled locally. To configure Port-Filter, run the **port-filter** command in control-plane configuration mode.

Configuration Example

1. Enable the Port-Filter function on the manage sub-interface:

```
FS(config)# control-plane manage
FS(config-cp)# port-filter
```

Verification

1. Run the **show ef-rnfp port-filter** command to check whether Port-Filter is enabled as well as the packet loss status.

Prompt

1. If no Port-Filter policy is configured on the data sub-interface, when the **no** or **default** operation is performed, a prompt will be displayed, indicating that the delete operation failed.

```
FS(config)# control-plane manage
FS(config-cp)# no port-filter
EF-RNFP:    delete port-filter rule failed
FS(config-cp)# default port-filter
EF-RNFP:    delete port-filter rule failed
```

3.11 scpp

Configure SCPP to conduct traffic differentiation and rate limit on each type of traffic according to policies: connection limit, semi-connection control, and traffic bandwidth limit.

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**]

Disable SCPP.

no scpp list *acl_no*

Restore the default configuration.

default scpp

Parameter Description

Parameter	Description
acl_no	Indicates the match policy. Matched traffic is differentiated and the rate is limited.
bw-rate *rate* **bw-burst-rate** *burst-rate*	Configures the rate limit and burst rate limit. The unit is pps.
conn-create-rate *create-rate* **conn-create-burst-rate** *create-burst-rate*	Configures the new connection rate and burst new connection rate.
conn-total *num*	Configures the allowable total number of connections.
log	Indicates whether logs are recorded.

Defaults

The SCPP function is disabled.

Command Mode

control-plane configuration mode. The function can be configured on the three sub-interfaces.

Default Level

14

Usage Guide

N/A

Configuration Example

On the manage sub-interface, for TCP protocol packet traffic initiated from the 192.168.52.0 network segment to the local mange sub-interface, set the rate limit to 100 pps, allowable burst rate limit to 150 pps, allowable total number of connections to 30, number of new connections per second to 5, and number of burst new connections per second to 7.

```
FS(config)# access-list 100 permit tcp 192.168.52.0 0.0.0.255 any

FS(config)# control-plane manage

FS(config-cp)# scpp list 100 bw-rate 100 bw-burst-rate 150 conn-create-rate 5 conn-create-burst-rate 7 conn-total 30
```

Verification

1. Run the **show ef-rnfp scpp manage** command to check whether SCPP is enabled on the manage sub-interface as well as the packet loss status.

Prompt

1. If no SCPP policy for the Access Control List (ACL) is configured on the sub-interface, an error will be displayed during deletion.

```
FS(config-cp)#no scpp lis 200

EF-RNFP:    delete scpp rule failed
```

Common Errors

3.12 security deny

Forbid users to telnet to the device and access the Web page of the device.

security deny { **lan-ping** | **lan-web** | **wan-ping** | **wan-web** | **lan-telnet-ssh** | **lan-snmp** | **wan-telnet-ssh** | **wan-snmp** }

Disable the function.

no security deny { **lan-ping** | **lan-web** | **wan-ping** | **wan-web** | **lan-telnet-ssh** | **lan-snmp** | **wan-telnet-ssh** | **wan-snmp** }

Restore the default configuration.

default security deny { **lan-ping** | **lan-web** | **wan-ping** | **wan-web** | **lan-telnet-ssh** | **lan-snmp** | **wan-telnet-ssh** | **wan-snmp** }

Parameter Description

Parameter	**Description**
lan-ping	Forbids intranet users to ping the device.
lan-web	Forbids intranet users to access the Web page of the device.
wan-ping	Forbids extranet users to ping the device.
wan-web	Forbids extranet users to access the Web page of the device.
lan-telnet-ssh	Forbidding intranet users to telnet to the device or log in to the device in SSH mode.
lan-snmp	Forbids the intranet server to manage the device over SNMP.
wan-telnet-ssh	Forbidding extranet users to telnet to the device or log in to the device in SSH mode.
wan-snmp	Forbids the extranet server to manage the device over SNMP.

Defaults

The function is disabled.

Command Mode

control-plane configuration mode

Default Level

14

Usage Guide

For common Ping and Web attack behaviors in the network, the function 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. The **no** option in this command can be used to delete related configuration.

Configuration Example

1. Forbid intranet PCs to ping the device.

```
FS(config)# control-plane
FS(config-cp)# security deny lan-ping
```

2. Forbid intranet PCs to log in to the Web page of the device.

```
FS(config)# control-plane

FS(config-cp)# security deny lan-web
```

3. Forbid the intranet server to manage the device over SNMP.

```
FS(config)# control-plane

FS(config-cp)# security deny lan-snmp
```

4. Forbid intranet PCs to log in to the Web page of the device.

```
FS(config)# control-plane

FS(config-cp)# security deny lan-telnet-ssh
```

Verification 1. Run the **show run** command to display the related configuration.

Platform Description 11.1PJ19MSC products do not support this command in bridge mode.

3.13 security web permit

Configure whitelisted users.

security web permit *low-ip-address* [*high-ip-address*]

Delete whitelisted users.

no security web permit *low-ip-address* [*high-ip-address*]

Restore the default configuration.

default security web permit *low-ip-address* [*high-ip-address*]

Parameter Description

Parameter	Description
low-ip-address	Indicates the allowable IP address or the start IP address of the allowable IP address range.
high-ip-address	Indicates the end IP address of the allowable IP address range.

Defaults The function is disabled.

Command Mode control-plane configuration mode

Default Level 14

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

1. Configure the IP address range 192.168.1.2-192.168.1.100 as whitelisted users.

```
FS(config)# control-plane
FS(config-cp)# security web permit 192.168.1.2 192.168.1.100
```

Verification

1. Run the **show ef-rnfp web-permit-ip** command to display the configured whitelisted users.

3.14 show arp-suspect

Display the ARP spoofing suspect list.

show arp-suspect

Parameter Description

Parameter	Description
arp-suspect	Displays the hosts added to the ARP spoofing suspect list.

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode

Default Level

14

Usage Guide

Run this command to display the list of ARP spoofing suspects detected by the device.

Configuration Example

1. Display the list of ARP spoofing suspects detected by the device.

```
FS#FS#show arp-suspect
IP address      MAC address
1.1.1.1         00d0.1234.5678
```

Field description:

Field	Description
IP address	Indicates the IP address of an ARP spoofing suspect.
MAC address	Indicates the MAC address of an ARP spoofing suspect.

Prompt

```
N/A
```

3.15 show attack-info

Display attack information about the device.

show attack-info { **current** | **history** }

Parameter

Parameter	Description

Description

current	Displays current attack information about the system.
history	Displays historical attack information about the system.

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode

Default Level

14

Usage Guide

Run this command to check whether the device is being attacked as well as the attack history.

Configuration Example

1. Displayall PIM interfaces.

```
FS# show attack-info history
System attack record at 1970-1-5 15:37:4, System in attack 8s
ALL:    1514 packets, 141600 bytes
PROTOCOL              packets            bytes
ARP                   2                  120
UDP                   1512               141480
TOP4 IP attack:
IP                    packets            bytes              interface
172.18.3.58         1500               138000             Gi0/1
100.100.100.73      10                 2982               Gi0/1
10.10.3.1           2                  120                Gi0/1
172.18.3.81         2                  498                Gi0/1

System attack record at 1970-1-5 15:30:10, System in attack 6s
ALL:    259 packets, 25015 bytes
PROTOCOL              packets            bytes
ARP                   3                  180
UDP                   256                24835
TOP4 IP attack:
IP                    packets            bytes              interface
172.18.3.69         250                23000              Gi0/1
100.100.100.73      4                  1291               Gi0/1
172.18.3.110        3                  180                Gi0/1
172.18.3.22         2                  544                Gi0/1
```

3.16 show ef-rnfp

Display information about local anti-attack .

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** }

Parameter Description

Parameter	**Description**
acpp	Displays ACPP configuration and packet loss status.
data	Displays packet loss status of the data sub-interface.
manage	Displays packet loss status of the manage sub-interface.
protocol	Displays packet loss status of the protocol sub-interface.
scpp	Displays SCPP configuration and packet loss status.
glean-car	Displays Glean-CAR configuration and packet loss status.
port-filter	Displays Port-Filter configuration and packet loss status.
mpp	Displays MPP configuration and packet loss status.
all	Displays the ACPP, SCPP, Glean-CAR, Port-Filter, and MPP configuration and packet loss status on the three sub-interfaces.
web-permit-ip	Displays the local anti-attack whitelist.
anti-arp-spoof	Displays the configuration for ARP spoofing suspect detection.

Command Mode

Privileged EXEC mode, global configuration mode, interface configuration mode

Default Level

14

Usage Guide

Run this command to display the packet loss status and configuration.

Configuration Example

1. Display the ARP-CAR packet loss information.

```
FS# show ef-rnfp arp-car
ARP CAR information:
  Manage subinterface:    enable
    RULE:
      allow packet rate per source:    10(pps)
      log:    off
    STATISTIC:
      dropped 17000657 packets
```

Field description:

Field	**Description**
enable	Enables the function.
allow packet rate per source: x(pps)	Indicates that the allowable ARP rate of each source IP

	address is *x*.
log	Indicates whether logs are recorded.
dropped xxx packets	Indicates the number of lost packets.

4 SSH Commands

4.1 crypto key generate

Use this command to generate a public key to the SSH server.

crypto key generate { **rsa** | **dsa** }

Parameter Description

Parameter	Description
rsa	Generates an RSA key.
dsa	Generates a DSA key.

Defaults

By default, the SSH server does not generate a public key.

Command Mode

Global configuration mode

Usage Guide

When you need to enable the SSH SERVER service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command **enable service ssh-server** at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.

Only DSA/RSA authentication is available for one connection. Also, the key algorithm may differ in different client. Thus, it is recommended to generate both RSA and DSA keys so as to ensure connection with the portal server.

RSA has a minimum modulus of 512 bits and a maximum modulus of 2,048 bits; DSA has a minimum modulus of 360 bits and a maximum modulus of 2,048 bits. For some clients like SCP clients, a 768-bit or more key is required. Thus, it is recommended to generate the key of 768 bits or more.

A key can be deleted by using the **no crypto key generate** command. The **no crypto key zeroize** command is not available.

Configuration Examples

The following example generates an RSA key to the SSH server.

```
FS# configure terminal
FS(con fig)# crypto key generate rsa
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.
crypto key zeroize { **rsa** | **dsa** }	Deletes DSA and RSA keys and disables the SSH server function.

Platform Description

N/A

4.2 crypto key zeroize

Use this command to delete a public key to the SSH server.

crypto key zeroize { **rsa | dsa** }

Parameter Description

Parameter	Description
rsa	Deletes the RSA key.
dsa	Deletes the DSA key.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command deletes the public key to the SSH server. After the key is deleted, the SSH server state becomes DISABLE. If you want to disable the SSH server, run the **no enable service ssh-server** command.

Configuration Examples

The following example deletes a RSA key to the SSH server.

```
FS# configure terminal
FS(config)# crypto key zeroize rsa
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.
crypto key generate { **rsa | dsa** }	Generates DSA and RSA keys.

Platform Description

N/A

4.3 disconnect ssh

Use this command to disconnect the established SSH connection.

disconnect ssh [**vty**] *session-id*

Parameter Description

Parameter	Description
vty	Established VTY connection
session-id	ID of the established SSH connection, in the range from 0 to 35

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

You can disconnect a SSH connection by entering the ID of the SSH connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.

Configuration Examples

The following example disconnects the established SSH connection by specifying the SSH session ID.

```
FS# disconnect ssh 1
```

The following example disconnects the established SSH connection by specifying the VTY session ID.

```
FS# disconnect ssh vty 1
```

Related Commands

Command	Description
show ssh	Displays the information about the established SSH connection.
clear line vty *line_number*	Disconnects the current VTY connection.

Platform Description

N/A

4.4 ip scp server enable

Use this command to enable the SCP server function on a network device.

Use the **no** form of this command to restore the default setting.

ip scp server enable

no ip scp server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Secure Copy (SCP) enables an authenticated user to transfer files to/from a remote device in an encrypted way, with high security and guarantee.

Configuration Examples

The following example enables the SCP server function.

```
FS# configure terminal
FS(config)# ip scp server enable
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

4.5 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh authentication-retries *retry times*

no ip ssh authentication-retries

Parameter Description

Parameter	Description
retry times	Authentication retry times, ranging from 0 to 5

Defaults

The default is 3.

Command Mode

Global configuration mode

Usage Guide

User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to display the configuration of the SSH server

Configuration Examples

The following example sets the authentication retry times to 2.

```
FS# configure terminal
FS(config)# ip ssh authentication-retries 2
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

4.6 ip ssh cipher-mode

Use this command to set the SSH server encryption mode.

Use the **no** form of this command to restore the default setting.

ip ssh cipher-mode { **cbc** | **ctr** | **others** }

no ip ssh cipher-mode

Parameter Description

Parameter	Description
cbc	Encryption mode: CBC (Cipher Block Chaining) Encryption algorithm: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blow fish-CBC
ctr	Encryption mode: CTR (Counter) Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR
others	Encryption mode: Others Encryption algorithm: RC4

Defaults

All encryption modes are supported by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to set the SSH server encryption mode.

For FS Networks, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports

AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. All these algorithms can be grouped into CBC, CTR and Other as shown above.

With the advancement of cryptography study, CBC and Others encryption modes are proved to easily decipher. It is recommended to enable the CTR mode to raise assurance for organizations and enterprises demanding high security.

Configuration Examples

The following example enables CTR encryption mode.

```
FS# configure terminal
FS(config)# ip ssh cipher-mode ctr
```

Platform Description

N/A

4.7 ip ssh hmac-algorithm

Use this command to set the algorithm for message authentication.

Use the **no** form of this command to restore the default setting.

ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96** }

no ip ssh hmac-algorithm

Parameter Description

Parameter	Description
md5	MD5 algorithm
md5-96	MD5-96 algorithm
sha1	SHA1 algorithm
sha1-96	SHA1-96 algorithm

Defaults

SSHv1: all the algorithms are not supported.

SSHv2: all the algorithms are supported.

Command Mode

Global configuration mode

Usage Guide

FS SSHv1 servers do not support algorithms for message authentication.

For FS Networks, the SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, MD5-96, SHA1, and SHA1-96 algorithms. Set the algorithm on your demand.

Configuration Examples

The following example sets the algorithm for message authentication to SHA1.

```
FS# configure terminal
FS(config)# ip ssh hmac-algorithm sha1
```

Platform Description

N/A

4.8 ip ssh peer

Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name.

Use the **no** form of this command to restore the default setting.

ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

no ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

Parameter Description

Parameter	Description
username	User name
filename	Name of a public key file
rsa	The public key is a RSA key
dsa	The public key is a DSA key

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets RSA and DSA key files associated with user **test**.

```
FS# configure terminal
FS(config)# ip ssh peer test public-key rsa flash:rsa.pub
FS(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description N/A

4.9 ip ssh time-out

Use this command to set the authentication timeout for the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh time-out *time*

no ip ssh time-out

Parameter Description

Parameter	Description
time	Authentication timeout, in the range from 1 to 120 in the unit of seconds

Defaults The default is 120 seconds.

Command Mode Global configuration mode

Usage Guide The authentication is considered timeout and failed if the authentication is not successful within 120 seconds starting from receiving a connection request. Use the **show ip ssh** command to display the configuration of the SSH server.

Configuration Examples

The following example sets the timeout value to 100 seconds.

```
FS# configure terminal
FS(config)# ip ssh time-out 100
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

4.10 ip ssh version

Use this command to set the version of the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh version { **1** | **2** }

no ip ssh version

Parameter Description

Parameter	Description
1	Supports the SSH1 client connection request.
2	Supports the SSH2 client connection request.

Defaults

SSH1 and SSH2 are compatible by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to configure the SSH connection protocol version supported by SSH server. By default, the SSH server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH server. Use the **show ip ssh** command to display the current status of SSH server.

Configuration Examples

The following example sets the version of the SSH server.

```
FS# configure terminal
FS(config)# ip ssh version 2
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

4.11 ipv6 ssh access-class

Use this command to set the IPv6 ACL filtering of the SSH server.

ipv6 ssh access-class *accessv6-list-name*

Use the **no** form of this command to delete the IPv6 ACL filtering of the SSH server.

no ipv6 ssh access-class

Parameter Description

Parameter	Description
accessv6-list-name	An IPv6 ACL name.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Run this command to perform IPv6 ACL filtering for all connections to the SSH server. In line mode, IPv6 ACL filtering is performed only for specific lines. However, IPv6 ACL filtering rules of the SSH are effective to all SSH connections.

Configuration Examples

The following example performs the IPv6 ACL filtering named testv6 for all connections to the SSH server.

```
FS# configure terminal
FS(config)# ipv6 ssh access-class testv6
```

Platform Description

N/A

4.12 show crypto key mypubkey

Use this command to display the information about the public key part of the public key to the SSH server.

show crypto key mypubkey { **rsa | dsa** }

Parameter Description

Parameter	Description
rsa	Displays the RSA key.
dsa	Displays the DSA key.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode

Usage Guide

This command is used to show the information about the public key part of the generated public key on the SSH server, including key generation time, key name, contents in the public key part, etc.

Configuration

The following example displays the information about the public key part of the public key to the SSH server.

Examples

```
FS(config)#show crypto key mypubkey rsa
% Key pair was generated at: 7:1:25 UTC Jan 16 2013
  Key name: RSA1 private
  Usage: SSH Purpose Key
  Key is not exportable.
  Key Data:
                AAAAAwEA AQAAAEEA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O Q10kz+4/
                /IgYR0ge 1sZNg32u dFEifZ6D zfLySPqC MTWLfw==

% Key pair was generated at: 7:1:25 UTC Jan 16 2013
  Key name: RSA private
  Usage: SSH Purpose Key
  Key is not exportable.
  Key Data:
                AAAAAwEA AQAAAEEA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi BbZGZvn3
                LEYYfQ9s pgYL0ZQf S0s/GY0X gJOMsc6z i8OAkQ==
```

Related Commands

Command	Description
crypto key generate { **rsa** | **dsa** }	Generates DSA and RSA keys.

Platform Description

N/A

4.13 show ip ssh

Use this command to display the information of the SSH server.

show ip ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode

Usage Guide

This command is used to display the information of the SSH server, including version, enablement state, authentication timeout, and authentication retry times.

If no key is generated for the SSH server, the SSH version is still unavailable even if this SSH version has been configured.

Configuration Examples

The following example displays the information of the SSH server.

```
SSH and SCP disabled:
FS(config)#show ip ssh
```

```
SSH Disable - version 1.99
please generate rsa and dsa key to enable SSH
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled

SSH and SCP enabled:
FS(config)#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: enabled
```

Related Commands

Command	Description
ip ssh version {**1** | **2**}	Configures the version for the SSH server.
ip ssh time-out time	Sets the authentication timeout for the SSH server.
ip ssh authentication-retries	Sets the authentication retry times for the SSH server.

Platform Description

N/A

4.14 show ssh

Use this command to display the information about the established SSH connection.

show ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode

Usage Guide

This command is used to display the information about the established SSH connection, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.

Configuration Examples

The following example displays the information about the established SSH connection:

```
FS#show ssh
Connection Version Encryption        Hmac           Compress    State                 Username
           0       1.5 blowfish                     zlib        Session started test
           1       2.0 aes256-cbc      hmac-sha1    zlib        Session started test
```

Field Description

Field	Description
Connection	VTY number
Version	SSH version
Encryption	Encryption algorithm
Hmac	Message authentication algorithm
Compress	Compress algorithm
State	Connection state
Username	Username

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5 DHCP Snooping Commands

5.1 clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP Snooping binding database.

clear ip dhcp snooping binding [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id* | **wlan** *wlan-id*]

Parameter Description

Parameter	Description
mac	Specifies the user MAC address to be cleared.
vlan-id	Specifies the ID of the VLAN to be cleared.
ip	Specifies the IP address to be cleared.
interface-id	Specifies the ID of the interface to be cleared.
wlan-id	Specifies the ID of the WLAN to be cleared.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear the current dynamic user information from the DHCP Snooping binding database.

After this command is used, all the DHCP clients connecting interfaces with IP Source Guard function enabled should request IP addresses again, or they cannot access network.

Configuration Examples

The following example clears the dynamic database information from the DHCP Snooping binding database.

```
FS# clear ip dhcp snooping binding
FS# show ip dhcp snooping binding
Total number of bindings: 0
MacAddress IpAddress Lease(sec) Type VLAN Interface
---------- ---------- ---------- -------- ---- ---------
```

Related Commands

Command	Description
show ip dhcp snooping binding	Displays the information of the DHCP Snooping binding database.

Platform Description

N/A

5.2 ip dhcp snooping

Use this command to enable the DHCP Snooping function globally.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping

no ip dhcp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

The **show ip dhcp snooping** command is used to display whether the DHCP Snooping function is enabled.

Configuration Examples

The following example enables the DHCP Snooping function.

```
FS# configure terminal
FS(config)# ip dhcp snooping
FS(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of DHCP Snooping.
ip dhcp snooping vlan	Configures DHCP Snooping enabled VLAN.

Platform Description

N/A

5.3 ip dhcp snooping bootp-bind

Use this command to enable DHCP Snooping BOOTP-bind function.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping bootp-bind

no ip dhcp snooping bootp-bind

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.

Configuration Examples

The following example enables the DHCP Snooping BOOTP-bind function.

```
FS# configure terminal
FS(config)# ip dhcp snooping bootp-bind
FS(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

5.4 ip dhcp snooping check-giaddr

Use this command to enable DHCP Snooping to support the function of processing Relay requests.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping check-giaddr

no ip dhcp snooping check-giaddr

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

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.

Configuration Examples

The following example enables DHCP Snooping to support the function of processing Relay requests.

```
FS# configure terminal
FS(config)# ip dhcp snooping check-giaddr
FS(config)# end
```

Related

Command	Description

Commands

show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform Description

N/A

5.5 ip dhcp snooping database

Use this command to configure file backup of the DHCP Snooping binding database.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping database sata0 [interval *time*]

no ip dhcp snooping database sata0

Parameter Description

Parameter	**Description**
time	Indicates the interval of storing the database in the unit of second. The range is from 10s to 86,400s. The default value is 300s.

Defaults

This function is disabled by default.

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.

Configuration Examples

The following example sets configures file backup of the DHCP Snooping binding database with the default interval.

```
FS# configure terminal
FS(config)# ip dhcp snooping database sata0
FS(config)# end
```

Related Commands

Command	**Description**
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.
show run	Displays the current backup mode.

Platform Description

N/A

5.6 ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP Snooping binding database into the flash periodically.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping database write-delay *time*

no ip dhcp snooping database write-delay

Parameter Description

Parameter	Description
time	The interval at which the system writes the dynamic user information of the DHCP Snooping database into the flash, in the range from 600 to 86,400 in the unit of seconds

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This function writes user information into flash in case of loss after restart. In that case, users need to obtain IP addresses again for normal communication.

ℹ Too fast writing will reduce flash durability.

Configuration Examples The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

```
FS# configure terminal
FS(config)# ip dhcp snooping database write-delay 3600
FS(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform Description N/A

5.7 ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

ip dhcp snooping database write-to-flash

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to write the dynamic user information of the DHCP binding database into flash in real time.

Configuration Examples

The following example writes the dynamic user information of the DHCP binding database into flash.

```
FS# configure terminal
FS(config)# ip dhcp snooping database write-to-flash
FS(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.8 ip dhcp snooping information option

Use this command to add option82 to the DHCP request message.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping information option [**standard-format**]

no ip dhcp snooping information option [**standard-format**]

Parameter Description

Parameter	Description
standard-format	The option82 uses the standard format.

Defaults

This function is disabled by default,

Command Mode

Global configuration mode

Usage Guide

This command adds option82 to the DHCP request messages based on which the DHCP server assigns IP addresses.

By default, this function is in extended mode.

DHCP Relay function adds option82 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping option82 and DHCP Relay at the same time.

Configuration Examples

The following example adds option82 to the DHCP request message.

```
FS# configure terminal
FS(config)# ip dhcp snooping information option
FS(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

5.9 ip dhcp snooping information option format remote-id

Use this command to set the option82 sub-option remote-id as the customized character string.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping information option format remote-id { **string** *ascii-string* **|** **hostname** }

no ip dhcp snooping information option format remote-id { **string** *ascii-string* **|** **hostname** }

Parameter Description

Parameter	Description
string *ascii-string*	The content of the option82 remote-id extension format is customized character string.
hostname	The content of the option82 remote-id extension format hostname

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command sets the remote-id in the option82 to be added to the DHCP request message as the customized character string. The DHCP server will assign the IP address according to the option82 information.

Configuration Examples

The following example adds the option82 into the DHCP request packets with the content of remote-id as hostname.

```
FS# configure terminal
FS(config)# ip dhcp snooping information option format remote-id hostname
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.10 ip dhcp snooping monitor

Use this command to enable DHCP Snooping monitoring.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping monitor

no ip dhcp snooping monitor

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

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 Examples The following example enables DHCP Snooping monitoring.

```
FS# configure terminal
FS(config)# ip dhcp snooping monitor
FS(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

5.11 ip dhcp snooping suppression

Use this command to set the port to be the suppression status.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping suppression

no ip dhcp snooping suppression

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode/WLAN security configuration mode

Usage Guide

This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request IP addresses through DHCP.

This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

Configuration Examples

The following example sets **fastethernet** 0/2 and WLAN 1 to be in the suppression status.

```
FS# configure terminal
FS(config)# interface fastEthernet 0/2
FS(config-if)# ip dhcp snooping suppression
FS(config-if)# end
FS# configure terminal
FS(config)# wlansec 1
FS(config-wlansec)# ip dhcp snooping suppression
FS(config-if-wlansec)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

5.12 ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to check the source MAC address of the DHCP request message. If the MAC address in the link-layer header is different from the CHADDR (Client MAC Address), the check fails ,and the packets will be discarded.

Configuration Examples

The following example enables the check of the source MAC address of the DHCP request message.

```
FS# configure terminal
FS(config)# ip dhcp snooping verify mac-address
FS(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

5.13 ip dhcp snooping vlan

Use this command to enable DHCP Snooping for the specific VLAN.

Use the **no** form of this command to restore the default setting.

ip dhcp snooping vlan {*vlan-rng* | { *vlan-min* [*vlan-max*] } }

no ip dhcp snooping vlan {*vlan-rng* | { *vlan-min* [*vlan-max*] } }

Parameter Description

Parameter	Description
vlan-rng	VLAN range of effective DHCP Snooping
vlan-min	Minimum VLAN of effective DHCP Snooping
vlan-max	Maximum VLAN of effective DHCP Snooping

Defaults

By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable DHCP Snooping for specified VLANs globally.

Configuration Examples

The following example enables the DHCP Snooping function in VLAN 1000.

```
FS# configure terminal
FS(config)# ip dhcp snooping vlan 1000
FS(config)# end
```

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP Snooping globally.

Platform Description

N/A

5.14 renew ip dhcp snooping database

Use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.

renew ip dhcp snooping database

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to import the flash file information to the DHCP Snooping database in real time.

ℹ Records out of lease time and repeated will be neglected.

Configuration Examples

The following example imports the flash file information to the DHCP Snooping database.

```
FS# renew ip dhcp snooping database
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.15 show ip dhcp snooping

Use this command to display the DHCP Snooping configuration.

show ip dhcp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the DHCP Snooping configuration.

```
FS# show ip dhcp snooping
Switch DHCP snooping status :ENABLE
Verification of hwaddr field status :DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                                   Trusted          Rate limit(pps)
------------------------             ----------------    ----------------
GigabitEthernet 0/4                        YES              unlimited
Default                                     No
```

Related Commands

Command	Description
ip dhcp snooping	Enables the DHCP Snooping globally.
ip dhcp snooping verify mac-address	Enables the check of source MAC address of DHCP Snooping packets.
ip dhcp snooping write-delay	Sets the interval of writing user information to FLASH periodically.
ip dhcp snooping information option	Adds option82 to the DHCP request message.
ip dhcp snooping bootp-bind	Enables the DHCP Snooping bootp bind function.
ip dhcp snooping trust	Sets the port as a trust port.

Platform Description N/A

5.16 show ip dhcp snooping binding

Use this command to display the information of the DHCP Snooping binding database.

show ip dhcp snooping binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display all the information of the DHCP Snooping binding database.

Configuration Examples

1: The following example displays the information of the DHCP Snooping binding database.

```
FS# show ip dhcp snooping binding
Total number of bindings: 1
NO.    MACADDRESS           IPADDRESS         LEASE(SEC)    TYPE              VLAN    INTERFACE
----- ------------------ --------------- ------------ ------------- ----- --------------------
1      0000.0000.0001     1.1.1.1          78128         DHCP-Snooping 1       GigabitEthernet 0/1
2      0000.0000.0002     2.2.2.2          78111         DHCP-Snooping 1       WLAN 1
```

Parameter	Description
Total number of bindings	The total number of bindings in the DHCP Snooping database.
NO.	The record order.
MacAddress	The MAC address of the user.
IpAddress	The IP address of the user.
Lease(sec)	The lease time of the record.
Type	The record type.
VLAN	The VLAN where the user belongs.
Interface	The user’s connection interface. It can be a either a wired access interface or wireless access WLAN.

Related Commands

Command	Description
ip dhcp snooping binding	Adds the static user information to the DHCP Snooping database.
clear ip dhcp snooping binding	Clears the dynamic user information from the DHCP Snooping binding database.

Platform Description

N/A

6 ARP-Check Commands

6.1 arp-check

Use this command to enable the ARP check function on the Layer 2 interface.

Use the **no** form of this command to restore the default setting.

arp-check

no arp-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command mode

Interface configuration mode/WLAN security configuration mode.

Usage Guide

The ARP check function generates the ARP filtering information according to legal user information, implementing the illegal ARP packet filtering on the network.

Configuration Examples

This following example enables the APR check function on interface GigabitEthernet 0/1.

```
FS# configure terminal
FS(config)# interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# arp-check
FS(config-if-GigabitEthernet 0/1)# end
FS# configure terminal
FS(config)# wlansec 1
FS(config-wlansec)# arp-check
FS(config-wlansec)# end
```

Related Commands

Command	Description
show interfaces arp-check list	Displays the ARP check entries.

Platform Description

N/A

6.2 show interfaces arp-check list

Use this command to display the ARP check entries on the Layer 2 interface.

show { **interface** [*interface-type interface-number*] | **wlan** [*wlan-id*] } **arp-check list**

Parameter

Parameter	Description

Description

interface-type	Wired interface type
interface-number	Wired interface number
wlan-id	WLAN ID

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the ARP check entries.

Configuration Examples

The following example displays the ARP check entries.

```
FS(config)#show interfaces arp-check list
INTERFACE                SENDER MAC     SENDER IP        POLICY SOURCE
------------------------ ---------------- ---------------- --------------------
GigabitEthernet 0/1          00D0.F800.0003      192.168.1.3          address-bind
GigabitEthernet 0/1          00D0.F800.0001      192.168.1.1          port-security
GigabitEthernet 0/4                               192.168.1.3          port-security
GigabitEthernet 0/5          00D0.F800.0003      192.168.1.3          address-bind
GigabitEthernet 0/7          00D0.F800.0006      192.168.1.6          AAA ip-auth-mode
GigabitEthernet 0/8          00D0.F800.0007      192.168.1.7          GSN
FS(config)#show wlan arp-check list
INTERFACE                    SENDER MAC          SENDER IP            POLICY SOURCE
------------------------ ---------------- ---------------- --------------------
WLAN 1                         00D0.F800.0008      192.168.1.8          GSN
```

Field	Description
INTERFACE	Interface name
SENDER MAC	Source MAC address
SENDER IP	Source IP address
POLICY SOURCE	Source of the entry

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7 IP Source Guard Commands

7.1 ip source binding

Use this command to add static user information to IP source address binding database.

Use the **no** form of this command to delete static user information from IP source address binding database.

ip source binding *mac-address* **{ vlan** *vlan-id* **}** *ip-address* { **interface** *interface-id* **| wlan** *wlan-id* **| ip-mac | ip-only** }

no ip source binding *mac-address* **{ vlan** *vlan-id* **}** *ip-address* { **interface** *interface-id* **| wlan** *wlan-id* **| ip-mac | ip-only** }

Parameter Description

Parameter	Description
mac-address	Adds user MAC address statically.
vlan-id	Adds user VLAN ID statically.
ip-address	Adds user IP address statically.
interface-id	Adds user interface ID statically.
wlan *wlan-id*	Add user WLAN ID statically.
ip-mac	The global binding type is IP+MAC
ip-only	The global binding type is IP only.

Defaults

No static address is added by default.

Command Mode

Global configuration mode

Usage Guide

This command allows specific clients to go through IP source guard detection instead of DHCP.

This command is supported on the wired L2 switching port, AP port, sub interface and WLAN.

This command enables global binding for IP source guard so that specific clients will get detected on all interfaces.

A static IPv6 source binding is valid either on wired and WLAN interfaces or in global configuration mode.

A new binding will overwrite the old one sharing the same configuration.

Configuration Examples

The following example adds the interface Id and WLAN ID of static users.

```
FS# configure terminal
FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface GigabitEthernet 0/1
FS(config)# ip source binding 0000.0000.0002 vlan 1 1.1.1.2 wlan 1
FS(config)# end
```

The following example adds static user information based on IP-MAC binding.

```
FS# configure terminal
FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
FS(config)# end
```

The following example adds static user information based on IP binding.

```
FS# configure terminal
FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only
FS(config)# end
```

Related Commands

Command	Description
show ip source binding	Displays the binding information of IP source address and database.

Platform Description

N/A

7.2 ip verify source

Use this command to enable IP Source Guard function on the interface.

Use the **no** form of this command to restore the default setting.

ip verify source [**port-security**]

no ip verify source

Parameter Description

Parameter	Description
port-security	Configures IP Source Guard to do IP+MAC-based detection.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode/WLAN security configuration mode

Usage Guide

This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection.

This command is supported on the wired L2 switching port, AP port, sub interface and WLAN.

IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.

Configuration Examples

The following example enables IP-based IP Source Guard function.

```
FS# configure terminal
FS(config)# interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ip verify source
FS(config-if)# end
FS(config)# wlansec 1
FS(config-wlansec)# ip verify source
FS(config-wlansec)# end
```

The following example enables IP+MAC-based IP Source Guard function.

```
FS# configure terminal
FS(config)# interface GigabitEthernet 0/2
FS(config-if-GigabitEthernet 0/2)# ip verify source port-security
FS(config-if)# end
FS(config)# wlansec 2
FS(config-wlansec)# ip verify source port-security
FS(config-wlansec)# end
```

Related Commands

Command	Description
show ip verify source	Displays user filtering entry of IP Source Guard.

Platform Description

N/A

7.3 ip verify source exclude-vlan

Use this command to exclude a VLAN from the IP source guard configuration on the port.

Use the **no** form of this command to restore the function.

ip verify source exclude-vlan *vlan-id*

no ip verify source exclude-vlan *vlan-id*

Parameter Description

Parameter	Description
vlan-id	The ID of VLAN excluded from the IP source guard configuration.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode/WLAN security configuration mode

Usage Guide

This command is used to exclude a VLAN from the IP source guard configuration. IP packets in this VLAN are forwarded without being checked and filtered.

Once the IP source guard function is disabled, the excluded VLAN is cleared automatically.

This command is supported on the wired L2 switching port, AP port, sub interface and WLAN.

Only when the IP source guard configuration is enabled on the port can a VLAN be excluded.

Configuration Examples

The following example configuration configures the IP source guard configuration for the port and excludes a VLAN.

```
FS# configure terminal
FS(config)# interface GigabitEthernet 0/1
FS(config-if-GigabitEthernet 0/1)# ip verify source
FS(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
FS(config-if)# end
FS(config)# wlansec 1
FS(config-wlansec)# ip verify source
FS(config-wlansec)# ip verify exclude-vlan 1
FS(config-wlansec)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.4 show ip source binding

Use this command to display the binding information of IP source addresses and database.

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*] [**wlan** *wlan-id*]

Parameter Description

Parameter	Description
ip-address	Displays user binding information of corresponding IP.
mac-address	Displays user binding information of corresponding MAC.
dhcp-snooping	Displays binding information of dynamic user.
static	Displays binding information of static user.
vlan-id	Displays user binding information of corresponding VLAN.
interface-id	Displays user binding information of corresponding interface.
wlan-id	Displays user information bound with the corresponding WLAN.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the binding information of IP source guard addresses and database.

```
FS# show ip source binding static
FS#show ip source binding static
Total number of bindings: 5
NO.   MACADDRESS          IPADDRESS         LEASE(SEC)   TYPE            VLAN   INTERFACE
----- ------------------ --------------- ------------ ------------- ----- --------------------
1     0001.0002.0001    1.2.3.2          Infinite     Static        1      Global
2     0001.0002.0002    1.2.3.3          Infinite     Static        1      GigabitEthernet 0/5
```

```
3      0001.0002.0003      1.2.3.4        Infinite     Static        1       Global
4      0001.0002.0004      1.2.3.5        Infinite     Static        1       Global
5      0001.0002.0005      1.2.3.6        Infinite     Static        1       WLAN 1
```

Related Commands

Command	Description
ip source binding	Sets the binding static user.

Platform Description

N/A

7.5 show ip verify source

Use this command to display user filtering entry of IP Source Guard.

show ip verify source [**interface** *interface-id*] [**wlan** *wlan-id*]

Parameter Description

Parameter	Description
interface-id	Displays user filtering entry of corresponding interface.
wlan-id	Displays user filtering entry of corresponding WLAN.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: “IP source guard is not configured on the interface FastEthernet 0/10”

Now, IP Source Guard supports the following filtering modes:

inactive-restrict-off: the IP Source Guard is disabled on bound interfaces.

inactive--not-apply: the IP Source Guard cannot adds bound entries into filtering entries for system errors.

active: the IP Source Guard is active.

Configuration Examples

The following example displays user filtering entry of IP Source Guard.

```
FS # show ip verify source
Total number of bindings: 7
NO.    INTERFACE                FILTERTYPE   FILTERSTATUS             IPADDRESS          MACADDRESS
VLAN TYPE
----- -------------------- ----------- ---------------------    --------------- --------------- -------- -------------
1        Global                   IP+MAC        Inactive-not-apply        192.168.0.127     0001.0002.0003    1
Static
2        GigabitEthernet 0/5    IP-ONLY        Active                    1.2.3.4           0001.0002.0004    1
DHCP-Snooping
3        Global                  IP-ONLY        Active                    1.2.3.7           0001.0002.0007    1
```

```
Static
4       Global              IP+MAC      Active                  1.2.3.6         0001.0002.0006   1
Static
5        GigabitEthernet  0/1    UNSET         Inactive-restrict-off    1.2.3.9         0001.0002.0009   1
DHCP-Snooping
6       GigabitEthernet 0/5   IP-ONLY      Active                 Deny-All
7       WLAN 1              IP-ONLY      Active                  Deny-ALL
```

Related Commands

Command	**Description**
ip verify source	Sets IP Source Guard on the interface.

Platform Description

N/A

8 VPDN Commands

8.1 accept dialin

Use this command to set the tunnel work mode to dial-in acceptance.

accept-dialin

Use the **no** form of this command to restore the default configuration of the system.

no accept-dialin

Parameter Description

Parameter	Description
N/A	N/A

Defaults No tunnel work mode is set for the system by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide No tunnel work mode is set for a VPDN-group by default. You must set the tunnel work mode first, and then set the tunnel work protocol and bound virtual template interface. The effective configuration or change of this command will immediately cause active and forcible disconnection of existing relevant tunnels.

Configuration Example #Set the tunnel work mode to dial-in acceptance.

```
FS(config)#vpdn-group 1
FS(config-vpdn)#accept-dialin
FS(config-vpdn-acc-in)#
```

Verification Run the **show running-config** command to check whether the tunnel work mode is dial-in acceptance.

N/A

The effective configuration or change of this command will immediately cause active and forcible disconnection of existing relevant tunnels.

N/A

8.2 authentication (L2TP)

Use this command to enable tunnel authentication.

Authentication

Use the **no** form of this command to restore the default configuration of the system.

no authentication

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Tunnel authentication is disabled by default.

Command Mode

L2TP-class interface configuration mode

Default Level

14

Usage Guide

You can enable or disable tunnel authentication as required.

Configuration Example

#Enable tunnel authentication.

```
FS(config)#l2tp-class 1
FS(config-l2tp-class)#authentication
FS(config-l2tp-class)#
```

Verification

Run the **show running-config** command to check whether tunnel authentication is enabled.

8.3 clear vpdn log

Use this command to clear user online/offline information in log files.

clear vpdn log

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command clears user online/offline information in log files.

Configuration Example

#Clear user online/offline information in log files.

```
FS# show vpdn log
Username                              IP          State   Online time          Offline time
user-1                             100.1.1.2     out    2014-11-16-14:09:04  2014-11-16-14:29:26
user-2                             100.1.2.2     out    2014-11-16-15:09:05  2014-11-16-16:09:27
```

```
FS# clear vpdn log
FS#
FS# show vpdn log
%No vpdn logs.
FS#
```

8.4 clear vpdn tunnel

Use this command to forcibly clear a specified tunnel.

clear vpdn tunnel [{ **l2tp** | **pptp** } [**id** *locid]* | [*remote-host-name*] **]**

Parameter Description

Parameter	Description
l2tp	Indicates an L2TP tunnel.
pptp	Indicates a PPTP tunnel.
remote-host-name	Indicates the peer host name of a tunnel.
locid	Indicates the ID of the tunnel to be deleted.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command forcibly clears a specified tunnel. If no parameter is set, all existing tunnels (including PPTP and L2TP tunnels) are forcibly cleared. If only a tunnel protocol is specified, the tunnels of the tunnel protocol are forcibly cleared. If a tunnel protocol and the peer host name of a tunnel are specified, tunnels whose peer host name matches the host name among tunnels of the tunnel protocol are forcibly cleared.

The ID of the tunnel to be deleted is **tunID** displayed after the **show vpdn** command is executed.

Configuration Example

#Clear all existing L2TP tunnels.

```
FS# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name     State    Remote Address    Port    Sessions L2TP Class/
VPDN Group
1        1        BLIZZARD     est       192.168.12.213    1701    1    1
LocID          RemID          TunID          Username, Intf/
State    Last Chg                                    Vcid, Circuit
1                 1                 1                 ms,Vi1                        est
00:46:30
%No active PPTP tunnels
FS# clear vpdn tunnel l2tp
FS#
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
%CHANGED: Interface Virtual-Access1, changed state to administratively down
```

```
FS# show vpdn
%No active L2TP tunnels
%No active PPTP tunnels
FS#
```

8.5 encapsulation (L2TP)

Use this command to set the data encapsulation mode for tunnels.

encapsulation l2tpv2

Parameter Description

Parameter	**Description**
l2tpv2	Transmits tunnel data via L2TP specified in RFC2661.

Defaults

No data encapsulation mode is set for tunnels by default.

Command Mode

Pseudowire-class interface configuration mode

Default Level

14

Usage Guide

On a pseudowire-class interface, set tunnel data transmission parameters only after setting the tunnel data encapsulation mode.

Configuration Example

#Set the tunnel data encapsulation mode to L2TPv2.

```

FS(config)#
FS(config)#pseudowire-class 1
FS(config-pw-class)#encapsulation l2tpv2
FS(config-pw-class)#
```

Verification

Run the **show running-config** command to display the data encapsulation mode of tunnels.

8.6 force-local-chap

Use this command to forcibly perform complete PPP authentication. When the client triggers the L2TP Access Concentrator (LAC) to start dialup, the LAC serves as the proxy of the L2TP Network Server (LNS) to authenticate the client. This command is used to re-authenticate the client after an L2TP tunnel is established. This command is available only on the LNS.

force-local-chap

Use the **no** form of this command to restore the default configuration of the system.

no force-local-chap

Parameter

Parameter	**Description**

Description

N/A	N/A

Defaults The LNS does not need to re-authenticate the client by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide Configure this command only after configuring the **vpdn enable** command.

Configuration Example #Configure PPP CHAP re-authentication for tunnels.

```
FS(config-vpdn)# force-local-chap
FS(config-vpdn)#
```

Verification Run the **show running-config** command to check whether the LNS conducts authentication on the client.

8.7 force-local-lcp

Use this command to forcibly perform complete PPP authentication. When the client triggers the LAC to dial up, the LAC serves as the proxy of the LNS to authenticate the client. This command is used to re-conduct LCP negotiation for the client after an L2TP tunnel is established. This command is available only on the LNS.

force-local-lcp

Use the **no** form of this command to restore the default configuration of the system.

no force-local-lcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults The LNS does not need to re-conduct LCP negotiation for the client by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide Configure this command only after configuring the **vpdn enable** command.

Configuration Example #Configure PPP LCP re-authentication for tunnels.

```
FS(config-vpdn)# force-local-lcp
FS(config-vpdn)#
```

Verification Run the **show running-config** command to check whether negotiation is conducted for the client.

8.8 hello

Use this command to set the transmission interval of Hello messages transmitted to keep L2TP tunnels alive.

hello *interval*

Use the **no** form of this command to restore the default configuration of the system.

no hello

Parameter Description

Parameter	Description
interval	Indicates the transmission interval of Hello messages in seconds. The value range is from 1 to 1,000.

Defaults The default transmission interval of Hello messages is 60 seconds.

Command Mode L2TP-class interface configuration mode

Default Level 14

Usage Guide You can set the transmission interval of Hello messages based on the network environment, to check whether an L2TP tunnel is still available. If the network is stable and reliable, set the transmission interval of Hello messages to a relatively large value.

Configuration Example #Set the transmission interval of Hello messages to 120 seconds.

```
FS(config-l2tp-class)# hello 120
FS(config-l2tp-class)#
```

Verification Run the **show running-config** command to display the transmission interval of Hello messages.

8.9 hostname (L2TP)

Use this command to set the local host name of an L2TP tunnel.

hostname *local-hostname-string*

Use the **no** form of this command to restore the default configuration of the system.

no hostname

Parameter Description

Parameter	Description
local-hostname-string	Indicates the local host name of a tunnel.

Defaults The system uses the router name as the local host name of a tunnel by default.

Command Mode L2TP-class interface configuration mode

Default Level 14

Usage Guide You can set the local host name of a tunnel as required to identify the tunnel. Any effective change on the local host name of a tunnel will cause active and forcible disconnection of the L2TP tunnel.

Configuration Example #Set the local host name of a tunnel to LAC.

```
FS(config-l2tp-class)# hostname LAC
FS(config-l2tp-class)#
```

Verification Run the **show running-config** command to display the local host name of the tunnel.

8.10 ip dfbit set

Use this command to disable tunnel data fragmentation for transmission.

ip dfbit set

Use the **no** form of this command to restore the default configuration of the system.

no ip dfbit set

Parameter Description

Parameter	Description
N/A	N/A

Defaults The system allows tunnel data fragmentation for transmission by default.

Command Mode Pseudowire-class interface configuration mode

Default Level 14

Usage Guide You can allow tunnel data fragmentation for transmission as required. Any effective change on the configuration of tunnel data fragmentation will immediately affect transmission of tunnel data but will not cause forcible disconnection of the L2TP tunnel.

Configuration Example #Disable tunnel data fragmentation for transmission.

```
FS(config-pw-class)# ip dfbit set
FS(config-pw-class)#
```

Verification Run the **show running-config** command to check whether tunnel data is fragmented for transmission.

8.11 ip local interface

Use this command to set the local (source) interface used by a tunnel.

ip local interface *interface-name*

Use the **no** form of this command to restore the default configuration of the system.

no ip local interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Indicates the name of a local interface.

Defaults The local (source) interface used by a tunnel is not specified by default.

Command Mode Pseudowire-class interface configuration mode

Default Level 14

Usage Guide You can specify a network interface on a router as the local (source) interface of a tunnel. Any effective change on the configuration of the local (source) interface of a tunnel will cause active and forcible disconnection of the L2TP tunnel.

Configuration Example #Set the local (source) interface of a tunnel to Serial 0.

```
FS(config-pw-class)# ip local interface serial 0
FS(config-pw-class)#
```

Verification Run the **show running-config** command to display the local (source) interface of the tunnel.

8.12 ip precedence

Use this command to set the precedence field in the IP header of tunnel packets.

ip precedence { *precedence-value* **| critical | flash | flash-override | immediate | internet | network | priority | routine** }

Use the **no** form of this command to restore the default configuration of the system.

no ip precedence

Parameter Description

Parameter	Description
precedence-value	Indicates the value of the precedence field. The value range is from 0 to 7.
critical	Indicates that the value of the precedence field is **5**.
flash	Indicates that the value of the precedence field is **3**.
flash-override	Indicates that the value of the precedence field is **4**.

immediate	Indicates that the value of the precedence field is **2**.
internet	Indicates that the value of the precedence field is **6**.
network	Indicates that the value of the precedence field is **7**.
priority	Indicates that the value of the precedence field is **1**.
routine	Indicates that the value of the precedence field is **0**.

Defaults The default value of the precedence field in the IP header of tunnel packets is **0**.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide Use this command if you need to set the priority of tunnel data. Effective configuration of this command will immediately affect transmission of tunnel data, but will not cause active or forcible disconnection of relevant tunnels.

Configuration Example #Set the priority of tunnel data to **7**.

```
FS(config-vpdn)# ip precedence 7
FS(config-vpdn)#
```

Verification Run the **show running-config** command to display the precedence field in the IP header of tunnel packets.

8.13 ip tos

Use this command to set the type of service (TOS) field in the IP header of tunnel packets.

ip tos { *tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min- monetary-cost** | **normal** | **reflect** }

Use the **no** form of this command to restore the default configuration of the system.

no ip tos

Parameter Description

Parameter	Description
tos-value	Indicates the value of the TOS field. The value range is from **0** to **15**.
max-reliability	Indicates that the value of the TOS field is **2**.
max-throughput	Indicates that the value of the TOS field is **4**.
min-delay	Indicates that the value of the TOS field is **8**.
min-monetary-cost	Indicates that the value of the TOS field is **1**.
normal	Indicates that the value of the TOS field is **0**.
reflect	Uses the TOS field in IP data packets carried by a tunnel as the TOS field in the IP header of tunnel packets.

Defaults

The default value of the TOS field in the IP header of tunnel packets is **0**.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide

Use this command if you need to set the TOS of tunnel data. Effective configuration of this command will immediately affect transmission of tunnel data, but will not cause active or forcible disconnection of relevant tunnels.

Configuration Example

#Set the TOS of tunnel data to **min-delay**.

```
FS(config-vpdn)# ip tos min-delay
FS(config-vpdn)#
```

Verification

Run the **show running-config** command to display the TOS field in the IP header of tunnel data.

8.14 ip ttl

Use this command to set the time to live (TTL) field in the IP header of tunnel packets.

ip ttl *ttl-value*

Use the **no** form of this command to restore the default configuration of the system.

no ip ttl

Parameter Description

Parameter	Description
ttl-value	Indicates the value of the TTL field. The value range is from 1 to 255.

Defaults

The TTL field in the IP header of tunnel packets is set to **255** by default.

Command Mode

Pseudowire-class interface configuration mode

Default Level

14

Usage Guide

You can set the TTL field in the IP header of tunnel packets as required. Any effective change on the configuration of the TTL field in the IP header of tunnel data will immediately affect transmission of tunnel data but will not cause forcible disconnection of the L2TP tunnel.

Configuration Example

#Set the TTL field in the IP header of tunnel packets to **253**.

```
FS(config-pw-class)# ip ttl 253
FS(config-pw-class)#
```

Verification Run the **show running-config** command to check whether the TTL field in the IP header of tunnel packets is set.

8.15 l2tp ip udp checksum

Use this command to calculate and fill in the UDP checksum field for L2TP tunnel packets.

l2tp ip udp checksum

Use the **no** form of this command to restore the default configuration of the system.

no l2tp ip udp checksum

Parameter Description

Parameter	Description
N/A	N/A

Defaults The UDP checksum field used in L2TP tunnel packets is null (that is, zero) by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide You can set whether to calculate and fill in the UDP checksum field used in L2TP tunnel packets as required. This command is available only after the **protocol l2tp** or **protocol any** command is configured.

Configuration Example #Specify the UDP checksum field in L2TP tunnel packets.

```
FS(config)#
FS(config)#vpdn-group 1
FS(config-vpdn)#accept-dialin
FS(config-vpdn-acc-in)#protocol any
FS(config-vpdn-acc-in)#exit
FS(config-vpdn)#l2tp ip udp checksum
FS(config-vpdn)#
```

Verification Run the **show running-config** command to check whether the UDP checksum field is used in L2TP data packets.

8.16 l2tp tunnel authentication

Use this command to enable tunnel authentication.

l2tp tunnel authentication

Use the **no** form of this command to restore the default configuration of the system.

no l2tp tunnel authentication

Parameter

Parameter	Description

Description

N/A	N/A

Defaults

Tunnel authentication is disabled by default.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide

You can enable or disable tunnel authentication as required. Any effective change on the configuration of the tunnel authentication function will cause active and forcible disconnection of relevant L2TP tunnels. This command is available only after the **protocol l2tp** or **protocol any** command is configured.

Configuration Example

#Enable tunnel authentication.

```
FS(config)#
FS(config)#vpdn-group 1
FS(config-vpdn)#accept-dialin
FS(config-vpdn-acc-in)#protocol any
FS(config-vpdn-acc-in)#exit
FS(config-vpdn)#l2tp tunnel authentication
FS(config-vpdn)#
```

Verification

Run the **show running-config** command to check whether tunnel authentication is enabled.

8.17 l2tp tunnel avp-hidden-compatible

Use this command to enable RFC2661-compliant AVP Hidden parsing algorithm. The system supports Cisco AVP hiding parsing algorithm by default.

l2tp tunnel avp-hidden-compatible-co

Use the **no** form of this command to restore the default configuration of the system.

no l2tp tunnel avp-hidden-compatible

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The system adopts Cisco AVP hiding parsing algorithm by default.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide You can enable or disable the RFC2661-compliant AVP hiding parsing algorithm as required. If two AVP hiding parsing algorithms need to be supported, you can configure multiple VPDN-groups. The configuration of this command does not affect the current L2TP tunnel.

Configuration Example #Enable RFC2661-compliant AVP hiding parsing algorithm.

```
FS(config-vpdn)# l2tp tunnel avp-hidden-compatible
FS(config-vpdn)#
```

Verification Run the **show running-config** command to check whether the system supports the RFC2661-compliant AVP hiding parsing algorithm.

8.18 l2tp tunnel force_ipsec

Use this command to configure the forcible IPSec packet encryption check. After this command is configured, only packets encrypted via IPSec can pass through VPDN tunnels.

l2tp tunnel force_ipsec

Use the **no** form of this command to restore the default configuration of the system.

no l2tp tunnel force_ipsec

Parameter Description

Parameter	Description
N/A	N/A

Defaults The forcible IPSec packet encryption check is disabled by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide You can enable or disable the forcible IPSec packet encryption check as required. Any effective change on the configuration of the forcible IPSec packet encryption check will cause active and forcible disconnection of relevant L2TP tunnels.

Configuration Example #Enable the forcible IPSec packet encryption check.

```
FS(config-vpdn)# l2tp tunnel force_ipsec
FS(config-vpdn)#
```

Verification Run the **show running-config** command to check whether packets must be encrypted before they are transmitted through VPDN tunnels.

8.19 l2tp tunnel hello

Use this command to set the transmission interval of Hello messages transmitted to keep a tunnel alive.

l2tp tunnel hello *interval*

Use the **no** form of this command to restore the default configuration of the system.

no l2tp tunnel hello

Parameter Description

Parameter	Description
interval	Indicates the transmission interval of Hello messages in seconds.

Defaults The default transmission interval of Hello messages is 60 seconds.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide You can set the transmission interval of Hello messages based on requirements and the network environment. Any effective change on the transmission interval of Hello messages of a tunnel will cause active and forcible disconnection of the L2TP tunnel.

Configuration Example #Set the transmission interval of Hello messages to 30 seconds.

```
FS(config-vpdn)# l2tp tunnel hello 30
FS(config-vpdn)#
```

Verification Run the **show running-config** command to display the transmission interval of Hello messages transmitted to keep the tunnel alive.

8.20 l2tp tunnel password

Use this command to set the tunnel authentication password.

l2tp tunnel password *password-string*

Use the **no** form of this command to clear the tunnel authentication password.

no l2tp tunnel password

Parameter Description

Parameter	Description
password-string	Indicates the tunnel authentication password.

Defaults No tunnel authentication password is set for the system by default.

Command VPDN-group interface configuration mode

Mode

Default Level 14

Usage Guide If tunnel authentication is required, tunnel authentication must be enabled and the same authentication password must be used at both ends of a tunnel. Any effective change on the tunnel authentication password will cause active and forcible disconnection of the relevant L2TP tunnel.

Configuration Example #Set the tunnel authentication password to **share**.

```
FS(config-vpdn)# l2tp tunnel password share
FS(config-vpdn)#
```

Verification Run the **show running-config** command to display the tunnel authentication password.

8.21 l2tp tunnel receive-window

Use this command to set the size of the receive window for tunnel control messages.

l2tp tunnel receive-window *size*

Use the **no** form of this command to restore the default configuration of the system.

no l2tp tunnel receive-window

Parameter Description

Parameter	Description
size	Indicates the size of the receive window for tunnel control messages.

Defaults The default size of the receive window for tunnel control messages is 4.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide Any changes on the size of the receive window for tunnel control messages will cause forcible disconnection of relevant L2TP tunnels.

Configuration Example #Set the size of the receive window for control messages to 12.

```
FS(config-vpdn)# l2tp tunnel receive-window 12
FS(config-vpdn)#
```

Verification Run the **show running-config** command to display the size of the receive window for tunnel control messages.

8.22 l2tp tunnel retransmit

Use this command to set retransmission parameters for L2TP tunnel control messages.

l2tp tunnel retransmit { retries *number* **| timeout { min | max }** *seconds* **}**

Use the **no** form of this command to restore the default configuration of the system.

no l2tp tunnel retransmit { **retries** | **timeout** { **min** | **max** } }

Parameter Description

Parameter	Description
number	Indicates the number of retransmission times of control messages.
seconds	Indicates the retransmission interval of control messages.

Defaults

The maximum number of retransmission times of control messages is 5, the minimum retransmission interval is 1 second, and the maximum retransmission interval is 8 seconds by default.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide

Any effective change on settings of retransmission parameters of tunnel control messages will cause active and forcible disconnection of relevant L2TP tunnels.

Configuration Example

#Set the maximum number of retransmission times of control messages to 10.

```
FS(config-vpdn)# l2tp tunnel retransmit retries 10
FS(config-vpdn)#
```

Verification

Run the **show running-config** command to display retransmission parameters of L2TP tunnel control messages.

8.23 l2tp tunnel timeout

Use this command to set the maximum waiting timeout period for establishing a session connection or control connection of an L2TP tunnel.

l2tp tunnel timeout { no-session | setup } *seconds*

Use the **no** form of this command to restore the default configuration of the system.

no l2tp tunnel timeout { **no-session** | **setup** }

Parameter Description

Parameter	Description
no-session	Indicates that a tunnel is established but the session connection is not established.
setup	Indicates that a control connection (tunnel) is not established.
seconds	Indicates the timeout period in seconds.

Defaults

The maximum allowable waiting timeout period for establishing a session connection is 600 seconds and the maximum allowable waiting timeout period for establishing a control connection (tunnel) is 300 seconds by default.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide

Any effective change on the maximum allowable waiting timeout period for establishing a session connection or control connection for an existing tunnel will cause active and forcible disconnection of the L2TP tunnel.

Configuration Example

#Set the allowable waiting timeout period for establishing a session connection of a tunnel to 1,200 seconds.

```
FS(config-vpdn)# l2tp tunnel timeout no-session 1200
FS(config-vpdn)#
```

Verification

Run the **show running-config** command to display the maximum allowable waiting timeout period for establishing a session connection or control connection of an L2TP tunnel.

8.24 l2tp-class

Use this command to set the L2TP-class interface of a specified name. If the L2TP-class interface of the specified name does not exist, the system creates an L2TP-class interface with the specified name.

l2tp-class *l2tp-class-name*

Use the **no** form of this command to delete the L2T-class interface of a specified name.

no l2tp-class *l2tp-class-name*

Parameter Description

Parameter	Description
l2tp-class-name	Indicates the name of an L2TP-class interface.

Defaults

No L2TP-class interface is set by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

You can configure or reference an L2TP-class interface to set work parameters for the L2TP control connection.

Configuration Example

#Create an L2TP-class interface named l2x.

```
FS(config)# l2tp-class l2x
FS(config-l2tp-class)#
```

Verification

Run the **show running-config** command to display the L2TP-class interface of the specified name.

8.25 lcp renegotiation always

Use this command to ignore errors in L2TP control packets that are from the peer device and do not comply with the RFC specifications, to ensure normal negotiation.

lcp renegotiation always

Use the **no** form of this command to restore the default configuration of the system.

no lcp renegotiation always

Parameter Description

Parameter	Description
N/A	N/A

Defaults Received L2TP control packets must strictly comply with specifications by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide Use this command to ignore errors in L2TP control packets that are from the peer device and do not comply with the RFC specifications, to ensure normal negotiation.

Configuration Example #Configure the function of ignoring errors in L2TP control packets that are from the peer device and do not comply with the RFC specifications.

```
FS(config-vpdn)# lcp renegotiation always
FS(config-vpdn)#
```

Verification Run the **show running-config** command to check whether errors in L2TP control packets that are from the peer device and do not comply with the RFC specifications are ignored.

8.26 local name

Use this command to set the local host name of a tunnel.

local name *local-hostname-string*

Use the **no** form of this command to restore the default configuration of the system.

no local name

Parameter Description

Parameter	Description
local-hostname-string	Indicates the local host name of a tunnel.

Defaults The system uses the router name as the local host name of a tunnel by default.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide

You can set the local host name for a tunnel on the router to identify the tunnel. The effective configuration or change of this command will immediately cause active and forcible disconnection of existing relevant tunnels.

Configuration Example

#Set the local host name of a tunnel to LNS.

```
FS(config-vpdn)# local name LNS
FS(config-vpdn)#
```

Verification

Run the **show running-config** command to display the local host name of the tunnel.

8.27 password (L2TP)

Use this command to set the tunnel authentication password.

password *password-string*

Use the **no** form of this command to restore the default configuration of the system.

no password

Parameter Description

Parameter	**Description**
password-string	Indicates the tunnel authentication password.

Defaults

Tunnel authentication is disabled by default and therefore no tunnel authentication password is set.

Command Mode

L2TP-class interface configuration mode

Default Level

14

Usage Guide

If tunnel authentication is required, tunnel authentication must be enabled and the same authentication password must be used at both ends of a tunnel. Any effective change on the tunnel authentication password will cause active and forcible disconnection of the relevant L2TP tunnel.

Configuration Example

#Set the tunnel authentication password to **share**.

```
FS(config-l2tp-class)# password share
FS(config-l2tp-class)#
```

Verification

Run the **show running-config** command to display the tunnel authentication password.

8.28 pptp flow-control receive-window

Use this command to set the maximum number of packets that are allowed to be sent before the peer device of a PPTP session receives the ACK from the local device.

pptp flow-control receive-window *packets*

Use the **no** form of this command to restore the default configuration of the system.

no pptp flow-control receive-window

Parameter Description

Parameter	Description
packets	Indicates the maximum number of packets that are allowed to be sent before the peer device of a PPTP session receives the ACK from the local device. The value range is from 1 to 64.

Defaults

The default value is 64 on the PNS and 16 on the PAC.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide

This command is a proprietary configuration command of PPTP. Therefore, this command is available only after the **protocol pptp** or **protocol any** command is configured.

According to recommendations in RFC2637 of PPTP, both parties of a session use half of the maximum receive window received from the peer device as the initial send window for the local device during negotiation. When the send window is full, the system stops sending packets to the peer device of the session, and reduces the size of the send window by half till the size of the send window becomes 1. The system resumes packet sending after receiving the ACK response to sent packets from the peer device. If no ACK timeout occurs after packets of the quantity equaling the size of the current send window are continuously sent to the peer device, the system increases the size of the local send window by 1 till the size is equal to the maximum receive window size of the peer device. The ACK timeout interval is calculated using a dedicated algorithm according to RFC2637. This command is available only after the **protocol pptp** or **protocol any** command is configured.

Configuration Example

#Set the maximum size of the receive window for local PPTP sessions to 32.

```
FS(config-vpdn)# accept-dialin
FS(config-vpdn-acc-in)# protocol pptp
FS(config-vpdn-acc-in)# exit
FS(config-vpdn)# pptp flow-control receive-window 32
FS(config-vpdn)#
```

Verification

Run the **show running-config** command to display the maximum number of packets that are allowed to be sent.

8.29 pptp flow-control static-rtt

Use this command to set the static reference timeout period for waiting the ACK response to a sent single data packet in a PPTP session.

pptp flow-control static-rtt *timeout-interval*

Use the **no** form of this command to restore the default configuration of the system.

no pptp flow-control static-rtt

Parameter Description

Parameter	Description
timeout-interval	Indicates the static reference timeout period in milliseconds for waiting the ACK response to a sent single data packet in a PPTP session. The value range is from 100 to 5,000.

Defaults The default value is 1500 milliseconds.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide This command is a proprietary configuration command of PPTP. Therefore, this command is available only after the **protocol pptp** or **protocol any** command is configured.

According to recommendations in RFC2637 of PPTP, the timeout interval for waiting the ACK response to sent PPTP packets, that is, the Acknowledgment Time-Out (ATO), is calculated using a dedicated algorithm, and the dynamically calculated Round-Trip Time (RTT) is used. **static-rtt** configured in this command is used as an initial reference value in RTT calculation.

Configuration Example #Set the static reference timeout period for waiting the ACK response to a sent single data packet in a PPTP session to 32 milliseconds.

```
FS(config-vpdn)# accept-dialin
FS(config-vpdn-acc-in)# protocol pptp
FS(config-vpdn-acc-in)# exit
FS(config-vpdn)# pptp flow-control static-rtt 32
FS(config-vpdn)#
```

Verification Run the **show running-config** command to display the static reference timeout period for waiting the ACK response to a sent single data packet in a PPTP session.

8.30 pptp tunnel echo

Use this command to set the interval for the local device of a PPTP tunnel for actively sending echo requests.

pptp tunnel echo *echo-packet-interval*

Use the **no** form of this command to restore the default configuration of the system.

no pptp tunnel echo

Parameter Description

Parameter	**Description**
echo-packet-interval	Indicates the interval in seconds for the local device of a PPTP tunnel for actively sending echo requests. The value range is from 0 to 1000.

Defaults

The default interval is 60 seconds.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide

This command is a proprietary configuration command of PPTP. Therefore, this command is available only after the **protocol pptp** or **protocol any** command is configured. When **echo-packet-interval** is set to **0**, the local device of a PPTP tunnel does not actively send echo packets.

When **echo-packet-interval** is not set to **0**, the local device of a PPTP tunnel actively sends an echo request to detect the tunnel status and starts a timer for waiting for an echo reply from the peer device if it fails to receive any valid protocol or data packet from the peer device within the interval specified by **echo-packet-interval**. The initial waiting timeout period is 1 second. If timeout occurs during waiting for the first echo reply, the local device of the PPTP tunnel sends the second echo request and doubles the waiting timeout period, and by analogy. If the local device fails to receive the echo reply from the peer device within five intervals, the device considers that the tunnel communication is abnormal, and disables the tunnel as well as sessions carried on the tunnel. This command is available only after the **protocol pptp** or **protocol any** command is configured.

Configuration Example

#Set the interval for the local device of a PPTP tunnel for sending echo requests to 30 seconds.

```
FS(config-vpdn)# accept-dialin
FS(config-vpdn-acc-in)# protocol pptp
FS(config-vpdn-acc-in)# exit
FS(config-vpdn)# pptp tunnel echo 30
FS(config-vpdn)#
```

Verification

Run the **show running-config** command to display the interval for the local device of a PPTP tunnel for actively sending echo requests.

8.31 protocol

Use this command to set a tunnel protocol for a tunnel.

protocol { **any** | **l2tp** | **pptp** }

Use the **no** form of this command to restore the default configuration of the system.

no protocol

Parameter Description

Parameter	**Description**
any	Matches all available tunnel protocols.
l2tp	Matches L2TP.
pptp	Matches PPTP.

Defaults

No tunnel protocol is specified for a tunnel by default.

Command Mode

VPDN-group interface configuration mode

Default Level

14

Usage Guide

You must specify a tunnel protocol for a tunnel. Any effective setting of or change on the tunnel protocol will cause active disconnection of existing relevant tunnels. This command is available only after the **accept-dialin** command is configured.

Configuration Example

#Set the tunnel protocol to L2TP.

```
FS(config-vpdn)# accept-dialin
FS(config-vpdn-acc-in)# protocol l2tp
FS(config-vpdn-acc-in)#
```

Verification

Run the **show running-config** command to display the tunnel protocol used by the tunnel.

8.32 protocol (L2TP)

Use this command to set L2TP control connection parameters.

protocol *l2tpv2* [*l2tp-class-name*]

Use the **no** form of this command to restore the default configuration of the system.

no protocol

Parameter Description

Parameter	**Description**
l2tpv2	Uses L2TP as the tunnel protocol.
l2tp-class-name	Indicates the name of a referenced L2TP-class interface.

Defaults

The system uses L2TPv2 as the L2TP tunnel protocol by default.

Command Mode

Pseudowire-class interface configuration mode

Default Level

14

Usage Guide

Any effective change on control connection parameters will cause active and forcible disconnection of the L2TP tunnel.

Configuration Example

#Set the tunnel protocol to L2TPv2 and apply the L2TP-class interface named l2x to set control connection parameters.

```
FS(config-pw-class)# protocol l2tpv2 l2x
FS(config-pw-class)#
```

Verification

Run the **show running-config** command to display L2TP control connection parameters.

8.33 pseudowire

Use this command to configure pseudowire rules.

Pseudowire *peer-ip-address vcid* { **encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }

Use the **no** form of this command to restore the default configuration of the system.

no pseudowire

Use this command to configure pseudowire rules using **hostname**.

pseudowire hostname *peer-hostname vcid* { **encapsulation** *l2tpv2* [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }

Use the **no** form of this command to restore the default configuration of the system.

no pseudowire

Parameter Description

Parameter	Description
peer-ip-address	Indicates the address of the remote L2TP network server (LNS).
peer-hostname	Indicates the host name that is registered by the LNS with the DNS server and that is maps to the address of the LNS.
vcid	Indicates the pseudowire global ID.
l2tpv2	Uses L2TPv2 (described in RFC 2661) as the tunnel protocol.
pw-class-name	Indicates the name of a referenced pseudowire-class unit.

Defaults

No pseudowire rule is configured by default.

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

Pseudowire rules can be configured only on the virtual-ppp interface. Any effective change on pseudowire rules of the virtual-ppp interface will cause active and forcible disconnection of relevant L2TP tunnels.

Configuration Example

#Configure a pseudowire rule on the virtual-ppp interface, and set the LNS address to 192.168.12.213 and reference the pseudowire-class interface named pw.

```
FS(config)# interface virtual-ppp 1
FS(config-if)# pseudowire 192.168.12.213 33 pw-class pw
FS(config-if)#
```

#Configure a pseudowire rule using the host name as follows:

Enable the DNS service, configure the address of the DNS server, and configure a route to the DNS server.

```
ip domain-lookup
l2tp-class 1
pseudowire-class 1
 encapsulation l2tpv2
ip name-server 192.168.5.119
ip name-server 61.154.22.41
interface FastEthernet 0/0
 ip ref
 ip address 192.168.52.90 255.255.255.0
 duplex auto
 speed auto
interface Virtual-ppp 1
 pseudowire hostname mm.hxs.meibu.com 1 encapsulation l2tpv2
 ppp pap sent-username user1 password    11
 ip address negotiate
ip route 0.0.0.0 0.0.0.0 192.168.52.1
```

Verification

Run the **show running-config** command to display pseudowire rules.

8.34 pseudowire-class

Use this command to set a pseudowire-class interface of a specified name. If the pseudowire-class interface of the specified name does not exist, the system creates a pseudowire-class interface with the specified name.

pseudowire-class *pseudowire-class-name*

Use the **no** form of this command to delete a pseudowire-class interface of a specified name.

no pseudowire-class *pseudowire-class-name*

Parameter Description

Parameter	Description
pseudowire-class-name	Indicates the name of a pseudowire-class interface.

Defaults

No pseudowire-class interface is set in the system by default.

Command Mode

Global configuration mode

Default Level 14

Usage Guide You can configure and reference a pseudowire-class interface to set L2TP tunnel work parameters.

Configuration Example #Create a pseudowire-class interface named pw.

```
FS(config)# pseudowire-class pw
FS(config-pw-class)#
```

Verification Run the **show running-config** command to display the pseudowire-class interface of the specified name.

8.35 receive-window

Use this command to set the size of the receive window for tunnel control messages.

receive-window *size*

Use the **no** form of this command to restore the default configuration of the system.

no receive-window

Parameter Description

Parameter	Description
size	Indicates the size of the receive window for control messages.

Defaults The default size of the receive window for control messages is 8.

Command Mode L2TP-class interface configuration mode

Default Level 14

Usage Guide Any effective change on the size of the receive window for tunnel control messages will cause active and forcible disconnection of the L2TP tunnel.

Configuration Example #Set the size of the receive window for control messages to 12.

```
FS(config-l2tp-class)# receive-window 12
FS(config-l2tp-class)#
```

Verification Run the **show running-config** command to display the size of the receive window for tunnel control messages.

8.36 retransmit

Use this command to set retransmission parameters for control messages.

retransmit {**initial** {**retries** *initial-retries* | **timeout** {**max** | **min**} *initial-timeout*} | **retries** *retries* | **timeout** {**max** | **min**} *timeout*}

Use the **no** form of this command to restore the default configuration of the system.

no retransmit { **initial** {**retries** | **timeout** {**max** | **min**} }| **retries** | **timeout** {**max** | **min**} }

Parameter Description

Parameter	Description
initial-retries	Indicates the number of SCCRQ retransmission times. The value range is from 1 to 1000.
initial-timeout	Indicates the SCCRQ retransmission interval. The value range is from 1 to 8.
retries	Indicates the number of retransmission times of other control messages. The value range is from 5 to 1000.
timeout	Indicates the retransmission interval of other control messages. The value range is from 1 to 8.

Defaults

By default, the number of SCCRQ retransmission times is 2, the number of retransmission times of other control messages is 5, and the minimum and maximum retransmission intervals of control messages are 1 second and 8 seconds respectively.

Command Mode

L2TP-class interface configuration mode

Default Level

14

Usage Guide

Any effective change on retransmission parameter settings of control messages will cause active and forcible disconnection of the L2TP tunnel.

Configuration Example

#Set the number of SCCRQ retransmission times to 3.

```
FS(config-l2tp-class)# retransmit initial retries 3
FS(config-l2tp-class)#
```

Verification

Run the **show running-config** command to display retransmission parameters of control messages.

8.37 show l2tp-class

Use this command to display the configuration information of a specified L2TP-class interface in the current system.

show l2tp-class [*l2tp-class-name*]

Parameter Description

Parameter	Description
l2tp-class-name	Specifies the name of an L2TP-class interface.

Defaults

N/A

Command Mode

Common user configuration mode and privileged EXEC mode

Default Level 14

Usage Guide You can use this command to display detailed configuration information of all L2TP-class interfaces or a specified L2TP-class interface configured in the system.

Configuration Example #Display the detailed configuration information of all L2TP-class interfaces in the current system.

```
FS# show l2tp-class
L2TP Class class-default:
    hidden disable, authentication disable
    hello interval 60 second(s)
    hostname Router, password Router
    timeout setup 120 seconds
    receive-window 8, no cookie space
    retransmit retries 5, retransmit initial retries 2
    retransmit timeout max 8 second(s), retransmit timeout min 1 second(s)
    retransmit initial timeout max 8 second(s)
    retransmit initial timeout min 1 second(s)

L2TP Class l2x:
    hidden disable, authentication disable
    hello interval 60 second(s)
    hostname Router, password Router
    timeout setup 120 seconds
    receive-window 8, no cookie space
    retransmit retries 5, retransmit initial retries 2
    retransmit timeout max 8 second(s), retransmit timeout min 1 second(s)
    retransmit initial timeout max 8 second(s)
    retransmit initial timeout min 1 second(s)
FS#
```

#Display the detailed configuration information of the L2TP-class interface of a specified name.

```
FS# show l2tp-class l2x
L2TP Class l2x:
    hidden disable, authentication disable
    hello interval 60 second(s)
    hostname Router, password Router
    timeout setup 120 seconds
    receive-window 8, no cookie space
    retransmit retries 5, retransmit initial retries 2
    retransmit timeout max 8 second(s), retransmit timeout min 1 second(s)
    retransmit initial timeout max 8 second(s)
    retransmit initial timeout min 1 second(s)
```

```
reference count: 1
```

Field description:

Field	Description
hidden	Indicates whether attribute-value pairs (AVPs) are hidden. The value **disable** indicates that AVPs are not hidden.
authentication	Indicates whether tunnel authentication is supported. The value **disable** indicates that tunnel authentication is not supported.
hello interval	Indicates the interval for sending Hello packets.
timeout setup	Indicates the maximum allowable time for establishing a control connection.
receive-window	Indicates the size of the receive window for tunnel control messages.
retransmit retries	Indicates the number of retransmission times of control messages except SCCRQ.
retransmit initial retries	Indicates the number of retransmission times of SCCRQ packets.
retransmit timeout max	Indicates the maximum retransmission interval of control messages except SCCRQ.
retransmit timeout min	Indicates the minimum retransmission interval of control messages except SCCRQ.
retransmit initial timeout max	Indicates the maximum retransmission interval of SCCRQ packets.
retransmit initial timeout min	Indicates the minimum retransmission interval of SCCRQ packets.
reference count	Indicates the number of pseudowire-class interfaces associated with the L2TP-class interface.

8.38 show pseudowire-class

Use this command to display the configuration information of a specified pseudowire-class interface in the current system.

show pseudowire-class [*pseudowire-class-name*]

Parameter Description

Parameter	Description
l2tp-class-name	Indicates the name of a specified pseudowire-class interface.

Defaults

-

Command Mode

Common user configuration mode and privileged EXEC mode

Default Level

14

Usage Guide

You can use this command to display detailed configuration information of all pseudowire-class interfaces or a specified pseudowire-class interface configured in the current system.

Configuration Example

#Display the detailed configuration information of all pseudowire-class interfaces in the current system.

```
FS# show pseudowire-class

Pseudowire Class pw:
   encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
   ip dfbit set disable, ip pmtu disable, ip ttl 255
   ip tos reflect disable, ip tos value 0
   reference count: 1000

Pseudowire Class pw1:
   encapsulation l2tpv2
   ip dfbit set disable, ip pmtu disable, ip ttl 255
   ip tos reflect disable, ip tos value 0
   reference count: 0

Pseudowire Class pw2:
   encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
   ip dfbit set disable, ip pmtu disable, ip ttl 255
   ip tos reflect disable, ip tos value 0
   reference count: 0
FS#
```

#Display the detailed configuration information of a pseudowire-class interface of a specified name.

```
FS# show pseudowire-class pw

Pseudowire Class pw:
   encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
   ip dfbit set disable, ip pmtu disable, ip ttl 255
   ip tos reflect disable, ip tos value 0
   reference count: 1000
FS#
```

Field description:

Field	Description
encapsulation	Indicates the encapsulation protocol.
protocol	Indicates the adopted protocol.
l2tp-class	Indicates the associated L2TP-class interface.
ip dfbit	Indicates whether tunnel data fragmentation is allowed.
ip ttl	Indicates the TTL field in the IP header of tunnel packets.
ip tos	Indicates the TOS field in the IP header of tunnel packets.

reference count	Indicates the number of virtual-ppp interfaces associated with the pseudowire-class interface.

8.39 show vpdn

Use this command to display information about a specified VPDN tunnel in the current system.

show vpdn [session | tunnel [{ l2tp | pptp } *locid* **]]**

Parameter Description

Parameter	Description
session	Displays all sessions.
tunnel	Displays all tunnels.
l2tp *locid*	Displays details about the L2TP tunnel of a specified ID. The value range is from 1 to 65535.
pptp *locid*	Displays details about the PPTP tunnel of a specified ID. The value range is from 0 to 65535.

Defaults

N/A

Command Mode

Common user configuration mode and privileged EXEC mode

Default Level

14

Usage Guide

You can use this command to check VPDN tunnel information in the current system. If no parameter is specified, information about all VPDN tunnels and sessions in the current system will be displayed.

Note: The username length is arbitrary. Therefore, when the **show** command is executed, only the first 12-byte strings in usernames are displayed to ensure alignment in the display format. Usernames with the length beyond the 12 bytes are not displayed completely.

To display the full names of usernames, run the **show vpdn tunnel l2tp locid** and **show vpdn tunnel pptp locid** commands.

Configuration Example

#Display information about all VPDN tunnels in the current system.

```
FS# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name      State    Remote Address    Port    Sessions L2TP Class/
VPDN Group
4        77       BLIZZARD         est       192.168.12.213    1701    1             1
LocID          RemID          TunID           Username, Intf/          State    Last Chg
                                              Vcid, Circuit
1              1              4               ms,Vi1                   est      00:33:58
%No active PPTP tunnels
FS#
```

#Display information about all VPDN tunnels in the current system.

```
FS# show vpdn tunnel
L2TP Tunnel Information Total tunnels 1
LocID RemID Remote Name      State    Remote Address    Port    Sessions L2TP Class/
VPDN Group
4         77       BLIZZARD          est        192.168.12.213    1701    1              1
%No active PPTP tunnels
FS#
```

Display information about all VPDN sessions in the current system.

```
FS# show vpdn session
L2TP Session Information Total sessions 1
LocID          RemID          TunID          Username, Intf/          State    Last Chg
                                             Vcid, Circuit
1               1               4               ms,Vi1                          est       00:37:03
%No active PPTP tunnels
FS#
```

#Display details about a specified PPTP or L2TP tunnel.

Display details about the L2TP tunnel of a specified tunnel ID.

```
FS# show vpdn tunnel l2tp 4
L2TP tunnel locid 4 is up,remote id is 77, 1 active sessions
   Tunnel state is est
   Tunnel transport is UDP
   Remote tunnel name is BLIZZARD
      Internet Address 192.168.12.213, port 1701
   Local tunnel name is LNStest
      Internet Address 192.168.12.212, port 1701
   VPDN group for tunnel is 1
   Tunnel domain unknown
   ip mtu adjust disabled
   Control Ns 2, Nr 4
```

Display details about the PPTP tunnel of a specified tunnel ID.

```
FS#show vpdn tunnel
%No active L2TP tunnels
PPTP Tunnel Information Total tunnels 1
LocID Remote Name          State            Remote Address    Port    Sessions
2                              estbed            192.168.45.160    3077    1
FS#
FS#show vpdn tunnel pptp 2
PPTP tunnel id 2 is up, remote id is 0, 1 active session
   Tunnel state is estbed
   Remote tunnel name is
      Internet Address 192.168.45.160, port 3077
   Local tunnel name is
      Internet Address 192.168.45.161
```

Field description:

Field	Description
L2TP Tunnel	Indicates an L2TP tunnel.
Session Information	Indicates session information.
LocID	Indicates the ID of the local device.
RemID	Indicates the ID of the peer device.
TunID	Indicates the tunnel ID.
Username, Intf:	Indicates the username and interface.
State	Indicates a state.
Last Chg	Indicates the last change time.
Remote Address	Indicates the peer address.
Port	Indicates the port.

8.40 show vpdn log

Use this command to display user online and offline information in the current log file.

show vpdn log [user *username*]

Parameter Description

Parameter	Description
username	Specifies a username.

Defaults N/A

Command Mode Common user configuration mode and privileged EXEC mode

Default Level 14

Usage Guide You can use this command to display online and offline information of all users or a specified user in the current log file.

Configuration Example #Display online and offline information of all users in the current log file.

```
FS# show vpdn log
Username              IP          State      Online time              Offline time
user-1              100.1.1.2    out    2014-11-16-14:09:04  2014-11-16-14:29:26
user-2              100.1.2.2    out    2014-11-16-15:09:05  2014-11-16-16:09:27
user-3              100.1.3.2    out    2014-11-16-17:09:04  2014-11-16-18:09:26
user-4              100.1.4.2    in     2014-11-16-18:09:05
FS#
```

#Display online and offline information of a specified user in the current log file.

```
FS# show vpdn log user user-1
Username         IP          State        Online time           Offline time
```

```
user-1          100.1.1.2     out     2014-11-16-14:09:04    2014-11-16-14:29:26
FS#
FS#show vpdn log user FS
%No vpdn logs for username: FS.
FS#
```

Field description:

Field	Description
Username	Indicates the username.
IP	Indicates the peer IP address.
State	Indicates the current state.
Online time	Indicates the online time.
Offline time	Indicates the offline time.

8.41 source-ip

Use this command to set the local (source) address of a tunnel established using the current VPDN-group.

source-ip *A.B.C.D*

Use the **no** form of this command to restore the default configuration of the system.

no source-ip

Parameter Description

Parameter	Description
A.B.C.D	Indicates the local (source) address of a tunnel established using the current VPDN-group.

Defaults The system does not limit the local (source) address of a tunnel established using the VPDN-group by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide If the local (source) address is set globally for the VPDN function, the local (source) address of a tunnel established using the VPDN-group must be consistent with the global local (source) address. The effective configuration or change of this command will immediately cause active and forcible disconnection of existing relevant tunnels.

Configuration Example #Set the local address of the tunnel established using the current VPDN-group to 202.101.92.73.

```
FS(config-vpdn)# source-ip 202.101.92.73
FS(config-vpdn)#
```

Verification Run the **show running-config** command to display the local (source) address of a tunnel established using the current VPDN-group.

8.42 terminate-from

Use this command to specify the peer host name of a tunnel.

terminate-from hostname *remote-hostname-string*

Use the **no** form of this command to restore the default configuration of the system.

no terminate-from

Parameter Description

Parameter	Description
remote-hostname-string	Indicates the peer host name of a tunnel.

Defaults The peer host name of a tunnel is not set by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide You can use this command to limit the host name of users who access the device remotely. If the peer host name of a tunnel is not set, the VPDN-group will not limit the host name of users who access the device remotely. Any effective change on the peer host name of a tunnel will cause active and forcible disconnection of all existing tunnels established using the VPDN-group.

Configuration Example #Set the peer host name of a tunnel to LAC.

```
FS(config-vpdn)# terminate-from hostname LAC
FS(config-vpdn)#
```

Verification Run the **show running-config** command to display the peer host name of the tunnel.

8.43 timeout setup

Use this command to set the maximum allowable time for establishing a control connection.

timeout setup *seconds*

Use the **no** form of this command to restore the default configuration of the system.

no timeout setup

Parameter Description

Parameter	Description
seconds	Indicates the maximum allowable time in seconds for establishing a control connection. The value range is from 60 to 6,000.

Defaults The maximum allowable time for establishing a control connection is 120 seconds by default.

Command Mode L2TP-class interface configuration mode

Default Level 14

Usage Guide Any effective change on the maximum allowable time for establishing a control connection will cause active and forcible disconnection of the relevant L2TP tunnel.

Configuration Example #Set the maximum allowable time for establishing a control connection to 240 seconds.

```
FS(config-l2tp-class)# timeout setup 240
FS(config-l2tp-class)#
```

Verification Run the **show running-config** command to display the maximum allowable time for establishing a control connection.

8.44 virtual-template

Use this command to set the virtual template interface bound to the current VPDN-group.

virtual-template *number*

Use the **no** form of this command to restore the default configuration of the system.

no virtual-template

Parameter Description

Parameter	Description
number	Indicates the serial number of a virtual template interface. The value range is from 1 to 1200.

Defaults No virtual template interface is bound to the VPDN-group by default.

Command Mode VPDN-group interface configuration mode

Default Level 14

Usage Guide You can use this command to bind the virtual template interface to a VPDN group so as to set parameters for network interfaces that carry sessions. Any effective change on the virtual template interface bound to a VPDN-group will cause forcible disconnection of existing tunnels of the VPDN-group.

Configure this command only after configuring the protocol command. Otherwise, the command is unavailable.

Configuration Example #Bind Virtual Template Interface 1 to VPDN-group 1.

```

FS(config)#
FS(config)#vpdn-group 1
FS(config-vpdn)#accept-dialin
FS(config-vpdn-acc-in)#protocol any
FS(config-vpdn-acc-in)#virtual-template 1
FS(config-vpdn-acc-in)#
```

Verification

Run the **show running-config** command to display the virtual template interface bound to the current VPDN-group.

8.45 vpdn congestion_avoidanc

Use this command to enable VPDN congestion control.

vpdn congestion_avoidanc

Use the **no** form of this command to disable VPDN congestion control.

no vpdn congestion_avoidanc

Parameter Description

Parameter	Description
N/A	N/A

Defaults

VPDN congestion control is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

You can determine whether to enable congestion control based on the current network environment.

Configuration Example

#Enable VPDN congestion control.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# vpdn congestion_avoidanc
FS(config)#
```

Verification

Run the **show running-config** command to check whether VPDN congestion control is enabled.

8.46 vpdn enable

Use this command to enable the VPDN function.

vpdn enable

Use the **no** form of this command to disable the VPDN function.

no vpdn enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The VPDN function is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

The VPDN function is not required for client-initiated L2TP tunnels, but it needs to be enabled when the device running FSOS provides the LAC or LNS function, or the device running FSOS uses the PPTP or L2TP protocol. The effective configuration or change of this command will immediately cause active and forcible disconnection of existing relevant tunnels.

Configuration Example

#Enable the VPDN function.

```
FS#config
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# vpdn enable
FS(config)#
```

Verification

Run the **show running-config** command to check whether the VPDN function is enabled.

8.47 vpdn ignore_source

Use this command to ignore the VPDN source address check on packets sent from the peer device. After this command is configured, the source address match is not checked for data packets sent from the peer device.

vpdn ignore_source

Use the **no** form of this command to strictly check the source addresses of packet sent from the peer device.

no vpdn ignore_source

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The system checks the source address match of tunnel packets by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to ignore the VPDN source address check on packets sent from the peer device. After this command is configured, the source address match is not checked for data packets sent from the peer device. This command is available only to data forwarded rapidly.

Configuration Example

#Ignore the VPDN source address check on packets sent from the peer device.

```
FS(config)# vpdn ignore_source
FS(config)#
```

Verification

Run the **show running-config** command to check whether the function of ignoring VPDN source address check on packets sent from the peer device is enabled.

8.48 vpdn limit_rate

Use this command to set the maximum number of VPDN tunnels that can be established per second, that is, limit the establishment rate of VPDN tunnels.

vpdn limit_rate *rate_num*

Use the **no** form of this command to disable the VPDN connection rate limit.

no vpdn limit_rate

Parameter Description

Parameter	Description
rate_num	Indicates the number of tunnels that can be established per second. The value range is from 5 to 100.

Defaults

Devices of FSOS10.x do not limit the establishment rate of VPDN tunnels by default. Devices of FSOS11.x limits the establishment rate of VPDN tunnels by default and the default value is 15 tunnels per second.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

When the dial-in of excessive VPDN tunnels affects overall performance of the system, use this command to limit the number of VPDN tunnel dial-ins.

Configuration Example

#Set the number of tunnels that can be established per second to 50.

```
FS(config)# vpdn limit_rate 50
FS(config)#
```

Verification

Run the **show running-config** command to display the number of VPDN tunnels that can be established per second.

8.49 vpdn session-limit

Use this command to set the maximum number of VPDN sessions allowed by the current system.

vpdn session-limit *sessions*

Use the **no** form of this command to restore the default configuration of the system.

no vpdn session-limit

Parameter Description

Parameter	Description
sessions	Indicates the maximum number of VPDN sessions allowed by the system. The value range is from 1 to 300.

Defaults

The maximum number of sessions supported by the system is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

When the dial-in of excessive VPDN tunnels affects overall performance of the system, use this command to limit the number of VPDN tunnel dial-ins. You must run the **vpdn enable** command to enable the VPDN function first.

Configuration Example

#Set the maximum number of allowable sessions to 100.

```
FS(config)# vpdn session-limit 100
FS(config)#
```

Verification

Run the **show running-config** command to display the maximum number of VPDN sessions allowed by the current system.

8.50 vpdn source-ip

Use this command to set the VPDN local (source) address used by the current system.

vpdn source-ip *A.B.C.D*

Use the **no** form of this command to restore the default configuration of the system.

no vpdn source-ip *A.B.C.D*

Parameter Description

Parameter	Description
A.B.C.D	Indicates the VPDN local address used by the system.

Defaults

No VPDN local (source) address is set for the system by default.

Command Mode

Global configuration mode

Default Level 14

Usage Guide If the system provides the LNS (via L2TP) or home gateway (HGW) (via PPTP) function, you can use this command to limit the destination address in connection requests of all accepted tunnels to the preset address. The effective configuration or change of this command will immediately cause active and forcible disconnection of existing relevant tunnels. You must run the **vpdn enable** command to enable the VPDN function first.

Configuration Example #Set the destination address to be used in connection requests of all accepted tunnels to 192.168.12.223.

```
FS(config)# vpdn source-ip 192.168.12.223
FS(config)#
```

Verification Run the **show running-config** command to display the VPDN local (source) address used by the current system.

8.51 vpdn-group

Use this command to set a VPDN-group interface of a specified name. If the VPDN-group interface of the specified name does not exist, the system creates a VPDN-group interface with the specified name.

vpdn-group *vpdn-group-name*

Use the **no** form of this command to delete the VPDN-group interface of a specified name.

no vpdn-group *vpdn-group-name*

Parameter Description

Parameter	Description
vpdn-group-name	Indicates the name of a VPDN-group interface.

Defaults No VPDN-group interface is set by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide If the router needs to serve as an LNS or HGW, a VPDN-group interface must be created and set. You can use this command to manage VPDN-group interfaces. The deletion of a VPDN-group interface will directly cause active and forcible disconnection of existing tunnels. You must run the **vpdn enable** command to enable the VPDN function first.

Configuration Example #Create a VPDN-group interface named 1.

```
FS(config)#
FS(config)#vpdn enable
FS(config)#vpdn-group 1
FS(config-vpdn)#
```

Verification Run the **show running-config** command to display the VPDN-group interface of the specified name.

9 IPSEC-IKE Commands

9.1 authentication (IKE policy)

Use this command to specify the authentication method for IKE policies.

authentication { **pre-share** }

Use the **no** form of this command to restore the default configuration.

no authentication

Parameter Description

Parameter	Description
pre-share	Indicates pre-shared key authentication.

Defaults The pre-shared key authentication is used by default.

Command Mode IKE policy configuration mode

Default Level 14

Usage Guide Currently, IKE negotiation policies use the pre-shared key authentication by default.

Configuration Example #Configure an IKE policy with the priority of 10 and use pre-shared key authentication in the policy.

```
FS(config)# crypto isakmp policy 10
FS(isakmp-policy)#authentication pre-share
```

Verification N/A

9.2 clear crypto isakmp

Use this command to clear the currently running IKE security association (SA).

clear crypto isakmp [*connection-id*]

Parameter Description

Parameter	Description
connection-id	Indicates the ID of an IKE SA. All existing IKE SAs are cleared by default. The value range is from 0 to 65535.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide In general, only a specific IKE SA is cleared. Run the **show crypto isakmp sa** command to display the ID of the SA to be cleared, and then run the **clear crypto isakmp** command using the ID to clear the specific IKE SA.

Configuration Example #Clear all IKE SAs.

```
FS# clear crypto isakmp
```

9.3 clear crypto log

Use this command to clear IPSec VPN login and logout logs.

clear crypto log

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Example #Clear IPSec VPN login and logout logs.

```
FS # clear crypto log
```

N/A

```
FS # clear crypto log
ipsec is writing or reading log now, can not delete file
```

The command output shows that the IPSec process is writing data to or reading data from the log file, and therefore the log file cannot be deleted.

9.4 clear crypto sa

Use this command to clear an IPSec SA.

clear crypto sa

Use this command to clear an IPSec SA of the remote peer by IP address or host name.

clear crypto sa peer { *ip-address* | *peer-name* }

Use this command to clear an IPSec SA of the remote peer by encryption mapping name.

clear crypto sa map *map-name*

Use this command to clear an IPSec SA of the remote peer by IP address and security parameter index (SPI).

clear crypto sa spi *destination-address* { **ah** | **esp** } *spi*

Parameter Description

Parameter	Description
ip-address	Indicates the IP address of the remote peer.
peer-name	Indicates the host name of the remote peer.
map-name	Indicates the name of an encryption mapping set.
destination-address	Indicates the IP address of the local or remote peer.
spi	Specifies an SPI. The value range is from 0 to 4,294,967,295.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

5. The preceding commands are used to clear IPSec SAs. If the **peer**, **map**, and **SPI** keywords are not specified, all IPSec SAs will be deleted by default.
6. If an SA is established via IKE, the SA will be cleared. If IPSec activation packets are detected on an interface, IPSec renegotiates a new SA. If an SA is manually configured, the SA will be cleared and a new SA will be re-established.
7. New parameters are effective only to SAs negotiated after the parameter configuration but do not affect existing SAs. To make new parameters effective to existing SAs, run commands to clear existing SAs for SA re-negotiation.
8. The deletion of SAs will interrupt communication. To ensure that communication using other IPSec SAs is not interrupted, use the **peer**, **map**, and **SPI** keywords to specify a specific SA.
9. If only one SA is available or no data is communicated through other SAs, clear all SAs for SA re-negotiation.

Configuration Example

#Clear all IKE SAs.

```
FS# clear crypto sa
```

9.5 crypto dynamic-map

Use this command to create a dynamic encryption mapping entry and enter the encryption mapping configuration mode.

crypto dynamic-map *dynamic-map-name dynamic-seq-num*

Use the **no** form of this command to delete an encryption mapping set or entry.

no crypto dynamic-map *dynamic-map-name* [*dynamic-seq-num*]

Parameter Description

Parameter	Description
dynamic-map-name	Specifies the name of an encryption mapping set.
dynamic-seq-num	Specifies the ID of an encryption mapping entry. The value range is from 1 to 65,535.

Defaults No dynamic encryption mapping exists by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide

Configuration Example

Verification N/A

9.6 crypto IPSec df-bit

Use this command to set the DF value of the encapsulation header for all interfaces.

crypto IPSec df-bit { **clear** | **set** | **copy** }

Parameter Description

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 in the external header. The default value is **copy**.

Defaults This command is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide In IPSec tunnel mode, use the **clear** keyword in the command when you need to send packets with the size greater than the MTU or when you do not know the size of the MTU.

If this command is not enabled using a specific parameter, the device uses **copy** as the DF bit value by default.

Configuration Example #Zero out the DF bit of all interfaces.

```
FS(config)# crypto IPSec df-bit clear
```

Verification N/A

9.7 crypto IPSec multicast disable

Use this command to disable IPSec processing on multicast and broadcast packets.

crypto IPSec multicast disable

Use the **no** form of this command **to** enable IPSec processing on multicast and broadcast packets.

no crypto IPSec multicast disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults When this command is not configured and an ACL involves multicast and broadcast packets, the device conducts IPSec processing on the packets by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide If IPSec processing is not required for multicast and broadcast packets, configure this command to skip IPSec processing.

Configuration Example #Disable IPSec processing on multicast and broadcast packets.

```
FS(config)# crypto IPSec multicast disable
```

Verification N/A

9.8 crypto IPSec optional

Use this command to disable the IPSec security check.

crypto IPSec optional

Use the **no** form of this command to enable the IPSec security check.

no crypto IPSec optional

Parameter Description

Parameter	Description
N/A	N/A

Defaults The IPSec security check is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The security check consumes considerable resources. Disabling the security check can save CPU resources. In the L2TP over IPSec model, the IPSec security check can be forcibly enabled or only IPSec encrypted packets are allowed to pass through. For example, L2TP and IPSec encryption may be used together as required.

Configuration Example #Cancel the security check.

```
FS(config)# crypto IPSec optional
```

Verification N/A

9.9 crypto IPSec profile (global IPSec-profile)

Use this command to create or modify an encryption mapping set (profile).

crypto IPSec profile *profile-name*

Use the **no** form of this command to cancel an encryption mapping set (profile) or entry.

no crypto IPSec profile *profile-name*

Parameter Description

Parameter	Description
profile-name	Indicates the name of an encryption mapping set (profile).

Defaults No encryption mapping set is configured by default.

Command Mode Global configuration mode

Run this command to enter the profile encryption mapping configuration mode.

Default Level 14

Usage Guide When data encryption and protection are required on a tunnel interface, define an encryption mapping set (profile) and then apply it to the tunnel interface. Define encryption communication parameters in the encryption mapping set (profile). The parameters include the following:

10. IPSec security policies to be applied to communication: Select policies from the list composed of one or more transformation sets.
11. SA lifetime
12. Information about whether SAs are manually configured or established via IKE
13. Apply the encryption mapping set of a tunnel to the tunnel interface. In this way, all IP communication through the tunnel interface will be encrypted according to the encryption mapping set applied to the tunnel interface. After configuration is completed, the device automatically initiates IKE negotiation, or triggers IKE negotiation when receiving packets from this interface. Policies described in encryption mapping entries are used during SA negotiation. To ensure smooth IPSec communication between two IPSec peers, the encryption mapping entries of the tunnel between the two peers must contain compatible configuration statements. When two peers try to establish an SA, each of the peers must have one encryption mapping entry compatible with one

encryption mapping entry of the other peer, and the encryption mapping entry must meet at least the following conditions:

14. An encryption mapping entry must contain a compatible encryption access list (for example, image access list).
15. Encryption mapping entries of both peers must specify the peer address (unless the peer is using a dynamic encryption set).
16. The encryption mapping entries must share at least one identical transformation set.
17. Only one encryption mapping set is applied to a single interface. The encryption mapping set specifies IPSec/IKE.

Create multiple encryption mapping entries for one interface in either of the following cases:

1. Different data flows of the interface will be processed by different IPSec peers.
2. Different levels of IPSec security need to be applied to different types of communication (data sent to the same or different peers), for example, the communication between devices in one subnet needs to be authenticated while the communication between devices in another subnet needs to be authenticated and encrypted. In this case, different types of communication should be defined in two different ACLs, and one separate encryption mapping entry must be created for each encryption access list.

Configuration Example

#Complete the minimum configuration for an encryption mapping set (profile). The name of the profile is testprofile and the name of the transformation set is mytest.

```
FS(config)# crypto IPSec profile testprofile
FS(config-crypto-map)# set transform-set myset
```

Verification

N/A

9.10 crypto IPSec security-association lifetime

Use this command to change the global lifetime of an IPSec SA.

crypto IPSec security-association lifetime { **seconds** *seconds* | **kilobytes** *kilobytes* }

Use the **no** form of this command to restore the default value of lifetime.

no crypto IPSec security-association lifetime { **seconds** | **kilobytes** }

Parameter Description

Parameter	Description
seconds *seconds*	Indicates the SA timeout period in seconds. The default value is 3,600 (1 hour). It can be set to **0**, indicating that the timeout function is disabled. The value can be **0**, or any value from 120 to 86,400.
kilobytes *kilobytes*	Indicates the timeout communication amount of an SA in kilobytes. The default value is **4,608,000**. It can be set to **0**, indicating that the byte timeout function is disabled. The value can be **0**, or any value from 2,560 to 536,870,912.

Defaults

3,600 seconds (1 hour) and 4,608,000 KB (communication for 1 hour at the rate of 10 MB per second)

Command Mode

Global configuration mode

Default Level 14

Usage Guide

3. The communication encrypted using IPSec SAs uses shared keys. An SA times out after a period of time is reached or a certain communication amount is reached, so as to ensure security. Both ends need to re-negotiate an SA and use the new shared key. When devices negotiate an SA, the smaller value between the lifetime proposed by the peer and that configured on the local device is used as the lifetime of the new SA.
4. There are two lifetimes: time lifetime and communication amount lifetime. An SA times out whenever either lifetime expires first. If the global lifetime is changed, this change is effective only to new SAs that are negotiated after the change and does not affect existing SAs. To make the new settings take effect as soon as possible, run the **clear crypto sa** command to clear some or all content in the SA database.
5. To change the global time lifetime, run the **crypto IPSec security-association lifetime seconds** command. The time lifetime specifies that an SA times out after certain seconds. To change the global communication amount lifetime, run the **crypto IPSec security-association lifetime kilobytes** command. The communication amount lifetime specifies that an SA times out when the amount (in KB) of communication encrypted using the SA key reaches a certain amount.
6. A smaller lifetime indicates a lower probability of successful key cracking, because there is less data that is encrypted using the same key and that can be used by attackers for analysis. However, when the lifetime is shorter, it takes longer time for the CPU to establish a new SA. Manually configured SAs does not involve lifetime.
7. Lifetime work principle: After a certain period of time (specified by **seconds**) is reached or a certain data communication amount (specified by the **kilobytes** keyword) is reached, whichever is earlier, an SA (and relevant key) will time out. The negotiation of a new SA starts before the old SA lifetime expires. In this way, a new SA is available before the old SA times out. The negotiation of a new SA starts 30 seconds before the lifetime specified by the **seconds** keyword times out or 256 KB away from the amount lifetime of data communication carried by the tunnel (specified by the **kilobytes** keyword) expires, whichever is earlier. If no communication passes through a tunnel within the lifetime of an SA, no new SA will be negotiated when the SA times out. Likewise, the negotiation of a new SA starts only when IPSec needs to protect a packet.
8. The time lifetime and communication amount lifetime cannot be zero simultaneously. Otherwise, the negotiation will fail. The device does not check the local configuration and you need to confirm that the time lifetime and communication amount lifetime are not zero simultaneously.

Configuration Example

#Set the time lifetime to 2,500 seconds and communication amount lifetime to 2,304,000 KB (communication for half an hour at the rate of 10 MB) for IPSec SAs.

```
FS(config)# crypto IPSec security-association lifetime seconds 2500
FS(config)# crypto IPSec security-association lifetime kilobytes 2304000
```

Verification N/A

9.11 crypto IPSec security-association lifetime not_based_on initiator

Use this command to modify the negotiation match rule for lifetime in Phase 2 of IPSec. That is, the final negotiation result of lifetime in Phase 2 is the smaller value between the lifetime of the device in branch and that of the device in the headquarters.

crypto IPSec security-association lifetime not_based_on initiator

Use the **no** form of this command to restore the default match rule of lifetime in Phase 2. That is, the final negotiation result uses the lifetime of the device in the branch.

no crypto IPSec security-association lifetime { **seconds** | **kilobytes** }

Parameter Description

Parameter	Description
N/A	N/A

Defaults The final negotiation result of lifetime in Phase 2 uses the lifetime of the device in the branch by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide By default, the negotiation result of lifetime in Phase 2 uses the lifetime of the device in the branch, indicating that devices in both the headquarters and the branch use the lifetime of the branch as the lifetime in Phase 2. You can use the command to modify the match rule of the lifetime in Phase 2, so as to use the smaller value between the lifetime of the device in the headquarters and that of the device in the branch as the final negotiation result.

Configuration Example #Modify the match result of lifetime in Phase 2.

```
FS(config)# crypto IPSec security-association lifetime not_based_on initiator
```

Verification N/A

9.12 crypto IPSec security-association replay disable

Use this command to disable the replay function so as not to check retransmitted packets.

crypto IPSec security-association replay disable

Use the **no** form of this command to check retransmitted packets.

no crypto IPSec security-association replay disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Replay check is enabled by default. This command is not configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide After the command is executed to disable replay, packet retransmission is not checked, which can improve packet processing efficiency but increase the possibility of DoS attacks.

Configuration Example #Disable the packet retransmission check.

```
FS(config)# crypto IPSec security-association replay disable
```

Verification N/A

9.13 crypto IPSec transform-set

Use this command to define a transformation set for SAs.

crypto IPSec transform-set *transform-set-name transform1 [transform2 [transform3]]*

Use the **no** form of this command to delete a transformation set.

no crypto IPSec transform-set *transform-set-name*

Parameter Description

Parameter	Description
transform-set-name	Indicates the name of a transformation set.
transform1, transform2, transform3	Indicates the security protocol and algorithm used by an SA. For details, see the security configuration guide.

Defaults No transformation set is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide

1. A set is a combination of security protocols, algorithms, and other settings for 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 more of them in encryption mapping entries. Transformation sets defined in encryption mapping entries are used for IPSec SA negotiation, so as to protect data flows that match the ACL referenced in the 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.
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.

Configuration Example #Define a transformation set that uses the ESP-DES-MD5 protection mode (providing encryption and authentication services).

```
FS(config)# crypto IPSec transform-set myset esp-des esp-md5-hmac
```

Verification N/A

9.14 crypto isakmp enable

Use this command to enable IKE so as to use IKE to negotiate IPSec SAs.

crypto isakmp enable

Use the **no** form of this command to disable IKE.

no crypto isakmp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults IKE is enabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide IKE is enabled by default. If you need to use IKE for IPSec SA negotiation, this command is not required. If you do not use IKE for IPSec SA negotiation, use the **no** form of this command to disable IKE.

Configuration Example #Enable IKE.

```
FS(config)# crypto isakmp enable
```

Verification N/A

9.15 crypto isakmp keepalive

Use this command to send peer detection messages to the remote peer.

crypto isakmp keepalive *secs* [**on-demand | periodic**]

crypto isakmp keepalive *secs retries* [**on-demand | periodic**]

Use the **no** form of this command to disable the peer detection function.

no crypto isakmp keepalive

Parameter Description

Parameter	Description
secs	Indicates the keepalive duration of a tunnel in seconds. The value range is from 5 to 3600.
retries	Indicates the interval for retransmitting packets in seconds. The value range is from 2 to 60.

on-demand	Sends messages at the idle time of packet forwarding.
periodic	Sends messages at the configured interval.

Defaults No peer detection message is sent by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use the **crypto isakmp keepalive** command to enable the device to periodically send peer detection messages to the remote peer, to check whether the remote peer is alive.

Configuration Example #Set the tunnel keepalive duration to 60 seconds, packet retransmission interval to 5 seconds, and use the on-demand mode.

```
FS(config)# crypto isakmp    keepalive    60 5 on-demand
```

Verification N/A

9.16 crypto isakmp key

Use this command to specify the pre-shared key used in IKE negotiation.

crypto isakmp key { **0 | 7** } *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] }

Use the **no** form of this command to delete the specified pre-shared key.

no crypto isakmp key { **0 | 7**} *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] }

Parameter Description

Parameter	**Description**
0 | 7	Specifies a plaintext key or ciphertext key. **0** indicates a plaintext key and **7** indicates a ciphertext key.
keystring	Indicates the pre-shared key string. It can contain a maximum of 128 characters.
peer-hostname	Indicates the host name of the remote peer.
peer-address	Indicates the IP address of the remote peer.
mask	Specifies the subnet for a network segment address.

Defaults No pre-shared key is specified by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide In general, IKE uses a pre-shared key for negotiation. To enable IKE to successfully establish an IKE SA, 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.

Configuration Example

#Set the pre-shared key used for IKE negotiation with the peer at the IP address of 172.16.1.1 to **mysecret**.

```
FS(config)# crypto isakmp key 0    mysecret address 172.16.1.1
```

Verification

N/A

9.17 crypto isakmp limit disable

Use this command to disable the IKE negotiation rate limit function.

crypto isakmp limit disable

Use the **no** form of this command to enable the IKE negotiation rate limit function.

no crypto isakmp limit disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The IKE negotiation rate limit function is enabled by default and the negotiation rate is limited to 1000.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Disable the IKE negotiation rate limit function.

Configuration Example

#Disable the IKE negotiation rate limit function.

```
FS(config)# crypto isakmp limit disable
```

Verification

N/A

9.18 crypto isakmp limit rate

Use this command to limit the IKE negotiation rate, that is, limit the maximum number of tunnels that can be negotiated simultaneously.

crypto isakmp limit rate *numbers*

Use the **no** form of this command to cancel the rate limit and restore the default value.

no crypto isakmp limit rate

Parameter

Parameter	Description

Description

numbers	Indicates the limited rate.

Defaults

The limited rate is 1000 by default, indicating that 1000 IPSec tunnels can be negotiated simultaneously.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

When thousands of tunnels are negotiated simultaneously, the negotiation fails to converge or the convergence is slow. As a result, the entire negotiation takes several hours or even a longer time. For this, use this command to limit the negotiation rate, to ensure that the number of tunnels that are simultaneously negotiated is controlled to be within a certain range, thereby improving the negotiation efficiency.

Configuration Example

#Set the IKE negotiation rate.

```
FS(config)# crypto isakmp limit rate 500
```

Verification

N/A

9.19 crypto isakmp mode-detect

Use this command to enable the local security gateway to automatically use the aggressive mode for negotiation when it fails to complete IKE negotiation initiated by the peer in main mode.

crypto isakmp mode-detect

Use the **no** form of this command to disable the automatic aggressive mode.

no crypto isakmp mode-detect

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults

When this command is not configured, only the main mode is adopted for negotiation by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Many vendors set foot in security products but the implementation methods of security products from different vendors are different. Only two work modes are supported in Phase 1 of IKE negotiation. To ensure compatibility, use this command to automatically complete negotiation in aggressive mode when the IKE negotiation initiated by the peer cannot be completed.

Configuration Example

#Enable the device to automatically identify negotiation initiated in aggressive mode.

```
FS(config)# crypto isakmp mode-detect
```

Verification

N/A

9.20 crypto isakmp nat keepalive

Use this command to configure the interval for sending NAT keepalive messages.

crypto isakmp nat keepalive *secs*

Use the **no** form of this command to cancel the configured interval for sending NAT keepalive messages and restore the default transmission interval.

no crypto isakmp nat keepalive

Parameter Description

Parameter	Description
secs	Indicates the keepalive duration of a tunnel in seconds. The value range is from 5 to 3,600.

Defaults

The default value is 300 seconds.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

The device complies with RFC3947 and uses the IPSEC NAT-T technology and UDP header 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 (300 seconds) is used.

Configuration Example

#Set the interval for sending tunnel keepalive packets to 60 seconds.

```
FS(config)# crypto isakmp    nat keepalive    60
```

Verification

N/A

9.21 crypto isakmp nat-traversal disable

Use this command to disable the NAT traversal function.

crypto isakmp nat-traversal disable

Use the **no** form of this command to enable the NAT traversal function.

no crypto isakmp nat-traversal disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults NAT traversal is enabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The protocols for implementing the NAT traversal function supported by devices of some vendors may be incompatible. In special cases, disable the NAT traversal function to implement device interworking.

Configuration Example #Disable the NAT traversal function.

```
FS(config)# crypto isakmp nat-traversal disable
```

Verification N/A

9.22 crypto isakmp next-payload disable

Use this command to disable the next-payload check.

crypto isakmp next-payload disable

Use the **no** form of this command to enable the next-payload check.

no crypto isakmp next-payload disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, when DOI information cannot be identified, the device considers that the negotiation cannot continue and returns a failure message.

Command Mode Global configuration mode

Default Level 14

Usage Guide After the next-payload check is disabled, the DOI field that cannot be identified is ignored and the negotiation continues. However, if the reserved field is not **0** or the field length does not match the length range, a failure message is still returned.

Configuration #Disable the next-payload check.

Example

```
FS(config)# crypto isakmp next-payload disable
```

Verification N/A

9.23 crypto isakmp peer

Use this command to specify the first peer that initiates negotiation in the case of multiple peers.

crypto isakmp peer { bind | random }

Use the **no** form of this command to cancel the priority of the specified first peer that initiates negotiation.

no crypto isakmp peer

Parameter Description

Parameter	Description
bind	Binds peers with IPSec dialup peer addresses when multiple peer addresses are configured for a 3G card. This parameter takes effect only in 3G networks. The first dialup maps to the first peer according to the configured sequence.
random	Randomly selects the first peer that tries to initiate negotiation.

Defaults By default, the negotiation starts from the first peer according to the configured sequence.

Command Mode Global configuration mode

Default Level 14

Usage Guide When 3G links are used, if multiple dialup addresses configured for a 3G card map to peers in the IPSec mapping set, enable the peer binding function to accelerate dialup. Otherwise, the device needs to try multiple times to find the correct peer. It takes a long time to establish a tunnel for the first time.

Configuration Example

#Enable the function of randomly selecting the tunnel connection address.

```
FS(config)# crypto isakmp peer random
```

Verification N/A

9.24 crypto isakmp policy

Use this command to define an IKE policy of a certain priority and enter the IKE policy configuration mode.

crypto isakmp policy *priority*

Use the **no** form of this command to delete the policy of a certain priority.

no crypto isakmp policy *priority*

Parameter Description

Parameter	Description

priority	Indicates the priority of an IKE policy. The value is an integer in the range from 1 to 10,000, where **1** indicates the highest priority while **10,000** indicates the lowest priority.

Defaults There is no default priority.

Command Mode Global configuration mode

Default Level 14

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 is used. You can configure multiple IKE policies on the device. After the IKE negotiation starts, the device tries to search for the public policy configured at both ends, and the search starts from the policy with the specified highest priority on the remote peer.

Configuration Example #Configure an IKE policy with the priority of 100.

```
FS(config)# crypto isakmp policy 100
FS(isakmp-policy)# authentication pre-share
FS(isakmp-policy)# encryption des
FS(isakmp-policy)# group    2
FS(isakmp-policy)# hash    sha
```

Verification N/A

9.25 crypto isakmp vendorid disable

Use this command to disable the transmission of FS vendor ID information during IKE negotiation.

crypto isakmp vendorid disable

Use the **no** form of this command to enable the transmission of FS vendor ID information during IKE negotiation.

no crypto isakmp vendorid disable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, FS vendor ID information is transmitted during IKE negotiation.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Devices from some vendors cannot identify private vendor IDs during IKE negotiation, resulting in a negotiation failure. In this case, use this command to disable transmission of FS vendor ID information.

Configuration Example

#Disable transmission of vendor IDs during negotiation.

```
FS(config)# crypto isakmp vendorid disable
```

Verification

N/A

9.26 crypto map (global IPSec)

Use this command to create or modify an encryption mapping set.

crypto map *map-name seq-num* { ***ipsec-manual*** | ***ipsec-isakmp*** [**dynamic** *dynamic-map-name*] }

Use the **no** form of this command to cancel an encryption mapping set or entry.

no crypto map *map-name* [*seq-num*]

Parameter Description

Parameter	**Description**
map-name	Indicates the name of an encryption mapping set.
seq-num	Indicates the serial number of an encryption mapping entry. The value range is from 1 to 65535.
IPSec-manual	Specifies that a mapping entry is used for manually configuring IPSec SAs.
IPSec-isakmp	Specifies that a mapping entry is used for establishing IPSec SAs negotiated via IKE.
dynamic-map-name	Specifies the name of a dynamic encryption mapping set that is used as a policy template.

Defaults

No encryption mapping set is configured by default.

Command Mode

Global configuration mode

Run this command to enter the encryption mapping configuration mode.

Default Level

14

Usage Guide

To encrypt and protect data using IPSec, define an encryption mapping set and then apply it to a specific interface. Define encryption communication parameters in the encryption mapping set. The parameters include the following:

1. IPSec protection to be provided for communication: Associate a configured encryption access list.
2. Destination address of the communication protected via IPSec: Specify the remote IPSec peer.

3. Local address used for IPSec communication: Apply the encryption mapping set to an interface. IPSec uses the address of a communication interface as the address of the local peer.
4. IPSec security policies to be applied to communication: Select policies from the list composed of one or more transformation sets.
5. SA lifetime
6. Information about whether SAs are manually configured or established via IKE

Encryption mapping entries that share the same encryption mapping name but have different mapping SNs constitute one encryption mapping set. Apply the encryption mapping set to an interface. In this way, all IP communication through the interface will be checked according to the encryption mapping set applied to the interface. If outbound IP communication matches an encryption mapping entry and needs to be protected, and IKE is specified in the encryption mapping entry, the device negotiates an SA with the remote peer according to parameters specified in the encryption mapping entry. If manually configured SAs are specified in the encryption mapping entry, an SA must be configured during the configuration of the encryption mapping entry. Provided that an SA is successfully established, data will be encrypted for transmission regardless of whether the SA is manually configured or established via IKE. If the SA negotiation fails, data will be discarded.

Policies described in encryption mapping entries are used during SA association. To ensure smooth IPSec communication between two IPSec peers, the encryption mapping entries of the two peers must contain compatible configuration statements. When two peers try to establish an SA, each of the peers must have one encryption mapping entry compatible with one encryption mapping entry of the other peer, and the encryption mapping entry must meet at least the following conditions:

7. An encryption mapping entry must contain a compatible encryption access list (for example, image access list).
8. Encryption mapping entries of both peers must specify the peer address (unless the peer is using a dynamic encryption mapping set).
9. The encryption mapping entries must share at least one identical transformation set.
10. Only one encryption mapping set is applied to a single interface. The encryption mapping set specifies IPSec/IKE or the combination of IPSec and manually configured entries. To create multiple encryption mapping entries for a specified interface, use the **seq-num** parameter to rank these encryption mapping entries. A smaller value of **seq-num** indicates a higher priority.

Create multiple encryption mapping entries for one interface in either of the following cases:

11. Different data flows of the interface will be processed by different IPSec peers.
12. Different levels of IPSec security need to be applied to different types of communication (data sent to the same or different peers), for example, the communication between devices in one subnet needs to be authenticated while the communication between devices in another subnet needs to be authenticated and encrypted. In this case, different types of communication should be defined in two different ACLs, and one separate encryption mapping entry must be created for each encryption access list.

For use of dynamic encryption mapping, see the section "crypto dynamic-map".

Configuration Example

#Complete the minimum configuration for a manually configured IPSec SA.

```
FS(config)# crypto map mymap 3 IPSec-manual
FS(config-crypto-map)# set peer 2.2.2.2
FS(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890
FS(config-crypto-map)# set session-key outbound esp 300 cipher abcdef1234567890
FS(config-crypto-map)# set transform-set myset
FS(config-crypto-map)# match address 101
```

#Complete the minimum configuration for an IPSec SA negotiated via IKE.

```
FS(config)# crypto map mymap 4 IPSec-isakmp
FS(config-crypto-map)# set peer 2.2.2.2
FS(config-crypto-map)# set transform-set myset
FS(config-crypto-map)# match address 101
```

Verification N/A

9.27 crypto map (interface IPSec)

Use this command to apply a defined encryption mapping set to an interface.

crypto map *map-name*

Use the **no** form of this command to cancel the association between an interface and an encryption mapping set.

no crypto map [*map-name*]

Parameter Description

Parameter	Description
map-name	Indicates the name of an encryption mapping set.

Defaults No encryption mapping set is applied to an interface by default.

Command Mode Interface configuration mode

Default Level 14

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 have 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.

One encryption mapping set can be configured only on one interface.

Configuration Example #Apply the encryption mapping set named mymap to Interface s0.

```
FS(config)# interface   serial   0
FS(config-if)# crypto map mymap
```

Verification N/A

9.28 crypto map local-address

Use this command to specify the IPSec local address.

crypto map *map-name* **local-address** *interface-type interface-number*

Use the **no** form of this command to cancel the specified IPSec local address.

no crypto map *map-name* **local-address**

Parameter Description

Parameter	Description
map-name	Indicates the name of an IPSec encryption mapping set.
interface-type	Indicates the type of the interface of which the address is used as the IPSec local address.
interface-number	Indicates the serial number of the interface of which the address is used as the IPSec local address.

Defaults

The address of the outbound interface of IPSec data is used as the IPSec local address by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

If an encryption mapping set is applied to multiple interfaces and this command is not executed, the device running FSOS creates an IPSec SA for each interface with the same remote peer and the same ACL. The IP address of the interface that sends and receives encryption traffic is used as the local address by default. After this command is executed to specify the local address, if the same encryption mapping set is applied to multiple interfaces, only one IPSec SA is created for communication.

If multiple interfaces on one device support IPSec communication, use this command to specify the IPSec local address to facilitate management. In this way, the device running FSOS uses a fixed address to communicate with external routers.

In general, it is recommended to use the IP address of the loopback interface as the IPSec local interface.

Configuration Example

#Specify the address of the Loopback0 interface as the IPSec local address.

```
FS(config)# crypto map mymap local-address loopback 0
```

Verification

N/A

9.29 debug crypto engine

Use this command to enable the work status debugging function for the encryption card.

debug crypto engine

Use the **no** form of this command to disable the work status debugging function for the encryption card.

no debug crypto engine

Parameter

Parameter	Description

Description

N/A	N/A

Defaults

The debugging function is disabled by default.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Enable the work status debugging function for the encryption card.

```
FS# debug crypto engine
```

#Disable the work status debugging function for the encryption card.

```
FS# no debug crypto engine
```

9.30 debug crypto IPSec

Use this command to enable the debugging function for IPSec packet forwarding.

debug crypto IPSec

Use the **no** form of this command to disable the debugging function for IPSec packet forwarding.

no debug crypto IPSec

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The debugging function is disabled by default.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Enable the debugging function for IPSec packet forwarding.

```
FS# debug crypto IPSec
```

#Disable the debugging function for IPSec packet forwarding.

```
FS# no debug crypto IPSec
```

Debugging

1. Packet encryption and decryption event

Debugging Information	can not find sa 727130249, vrf 0
Description	The SA with the SPI 727130249 is not found in vrf 0.
Cause	If a received packet needs to be decrypted, IPSec searches for an SA by SPI and other information in the packet for decryption. If no SA is found, the prompt above is displayed. This case mostly occurs in 3G links. IPSec configurations at both ends are inconsistent due to link instability, that is, an SA exists at one end but no SA exists at the other end.
Handling Suggestion	If this case occurs frequently, configure the IPSec keepalive mechanism, that is, DPD.

ℹ VRF is not supported on EG products. VRF-related cases are for reference only.

Debugging Information	packet need encrypto but not!
Description	IPSec receives an unencrypted packet that is supposed to be encrypted.
Cause	The possible cause is that IPSec is configured only at one end. When receiving an unencrypted packet, the device on which IPSec is configured discards the packet.
Handling Suggestion	Check the configurations at both ends.

9.31 debug crypto isakmp

Use this command to enable the IKE debugging function.

debug crypto isakmp

Use the **no** form of this command to disable the IKE debugging function.

no debug crypto isakmp

Parameter Description

Parameter	Description
N/A	N/A

Defaults The debugging function is disabled by default.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Example #Enable the IKE debugging function.

```
FS# debug crypto isakmp
```

#Disable the IKE debugging function.

```
FS# no debug crypto isakmp
```

Debugging

2. Protocol packet event

Debugging Information	received packet from 9.9.9.1, (R) MM_SR1_WI2, MM_KEY_EXCH
Description	An IKE negotiation packet is received from 9.9.9.1 and the negotiation mode is main mode. When the packet is received, the local device has sent the first packet SR1 and is waiting for the second packet WI2 from the initiator.
Cause	Every function that processes received packets prints similar information during IKE negotiation.
Handling Suggestion	N/A

3. Policy matching event in Phase 1

Debugging Information	(main mode)process in I1:no fit sa attribute was accepted!
Description	When processing the first negotiation message I1 from the initiator, the receiver fails to find the proper Phase 1 policy configuration.
Cause	The Phase 1 policies configured on the receiver and initiator are inconsistent.
Handling Suggestion	Check whether IKE policy configurations at both ends are consistent.

4. Negotiation authentication event

Debugging Information	Check main mode hash payload fail!
Description	The IKE negotiation authentication fails in main mode.
Cause	The identity of the peer needs to be authenticated in the last phase of IKE negotiation. In pre-shared authentication mode, both parties need to use the configured pre-shared key to authenticate the peer.
Handling Suggestion	Check whether the pre-shared keys of both parties are consistent.

9.32 encryption (IKE policy)

Use this command to specify the encryption algorithm for IKE policies.

encryption { **des** | **3des | aes-128 | aes-192 | aes-256** }

Use the **no** form of this command to restore the default encryption algorithm.

no encryption

Parameter Description

Parameter	**Description**
des	Specifies the 56-bit DES-CBC as the encryption algorithm.

3des	Specifies the 168-bit DES-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.

Defaults The 56-bit DES-CBC encryption algorithm is used by default.

Command Mode IKE policy configuration mode

Default Level 14

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.

Configuration Example #Specify DES as the encryption algorithm for IKE policies.

```
FS(config)# crypto isakmp policy 10
FS(isakmp-policy)# encryption des
```

Verification N/A

9.33 group (IKE policy)

Use this command to specify the ID of the Diffie-Hellman group in IKE policies.

group { **1** | **2** | **5** }

Use the **no** form of this command to restore the default ID of the Diffie-Hellman group.

no group

Parameter Description

Parameter	Description
1	Indicates the 768-bit Diffie-Hellman group.
2	Indicates the 1024-bit Diffie-Hellman group.
5	Indicates the 1536-bit Diffie-Hellman group.

Defaults The 768-bit Diffie-Hellman group (group 1) is used by default.

Command Mode IKE policy configuration mode

Default Level 14

Usage Guide Use this command to specify the Diffie-Hellman group to be used in an IKE policy.

Configuration Example

#Specify the 1024-bit Diffie-Hellman group for an IKE policy.

```
FS(config)# crypto isakmp policy 10
FS(isakmp-policy)# group 2
```

Verification

N/A

Platform Description

9.34 hash (IKE policy)

Use this command to specify the hash algorithm for IKE policies.

hash { **sha | md5** }

Use the **no** form of this command to restore the default hash algorithm.

no hash

Parameter Description

Parameter	Description
sha	Specifies SHA-1 (HMAC variant) as the hash algorithm.
md5	Specifies MD5 (HMAC variant) as the hash algorithm.

Defaults

SHA is used as the hash algorithm by default.

Command Mode

IKE policy configuration mode

Default Level

14

Usage Guide

Use this command to specify the hash algorithm to be used in an IKE policy.

Configuration Example

#Specify MD5 as the hash algorithm.

```
FS(config)# crypto isakmp policy 10
FS(isakmp-policy)# hash md5
```

Verification

N/A

9.35 lifetime (IKE policy)

Use this command to specify the lifetime of IKE SAs.

lifetime *seconds*

Use the **no** form of this command to restore the default IKE SA lifetime.

no lifetime

Parameter Description

Parameter	Description
seconds	Indicates the IKE SA lifetime in seconds. The value is an integer in the range from 60 to 86,400.

Defaults The default value is 86,400 seconds (1 day).

Command Mode IKE policy configuration mode

Default Level 14

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 while a shorter lifetime indicates a lower cracking probability. Therefore, set a proper lifetime (for example, 43,200 seconds) as required.

Configuration Example #Set the IKE SA lifetime to 1,000 seconds.

```
FS(config)# crypto isakmp policy 10
FS(isakmp-policy)# lifetime 1000
```

Verification N/A

9.36 match address (IPSec)

Use this command to specify an ACL for an encryption mapping entry.

match address *access-list-number*

Use the **no** form of this command to delete an ACL from an encryption mapping entry.

no match address

Parameter Description

Parameter	Description
access-list-number	Indicates the ACL No. (100-199, 2000-2699, and 2900-3899). Encryption mapping entries use only IP extended ACLs.

Defaults No ACL is specified in encryption mapping entries.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide Use this command to specify an ACL for an encryption mapping entry. The device judges whether data needs to be protected via IPSec according to the ACL in encryption mapping entry.

The ACL specified by this command is applied to both outbound and inbound communication. 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.

Configuration Example #Associate ACL 101 with the encryption mapping set named mymap.

```
FS(config)# crypto map mymap 4 IPSec-isakmp
FS(config-crypto-map)# match address 101
```

Verification N/A

9.37 match any

Use this command to specify the local IP address/subnet mask (0.0.0.0/0.0.0.0) and peer IP address/subnet mask (0.0.0.0/0.0.0.0) of the interested flow.

match any

Use the **no** form of this command to cancel the specified interested flow with local IP address/subnet mask (0.0.0.0/0.0.0.0) and peer IP address/subnet mask (0.0.0.0/0.0.0.0).

no match any

Parameter Description

Parameter	Description
N/A	N/A

Defaults The interested flow is not the flow from the local IP address/subnet mask (0.0.0.0/0.0.0.0) to the peer IP address/subnet mask (0.0.0.0/0.0.0.0) by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide Use this command to specify the interested flow with the local IP address/subnet mask (0.0.0.0/0.0.0.0) and peer IP address/subnet mask (0.0.0.0/0.0.0.0) for an encryption mapping set (profile). The encryption mapping set (profile) is mainly used in IPSec over GRE and L2TP over IPSec.

If **match any** is configured in the encryption mapping set (profile) where IPSec over GRE is used, the interested flow negotiated in Phase 2 is the flow from the local IP address/subnet mask (0.0.0.0/0.0.0.0) to the peer IP address/subnet mask (0.0.0.0/0.0.0.0).

Configuration Example

#Configure the interested flow in the encryption mapping set (profile) named test.

```
FS(config)#crypto ipsec profile test
FS(config-crypto-profile)#match any
```

Verification

N/A

9.38 mode (IPSec)

Use this command to change the encryption transformation set mode.

mode { **tunnel** | **transport** }

Use the **no** form of this command to restore the default mode.

no mode

Parameter Description

Parameter	Description
tunnel	Sets the transformation set mode to tunnel mode.
transport	Sets the transformation set mode to transport mode.

Defaults

The tunnel mode is used by default.

Command Mode

Encryption transformation set configuration mode

Default Level

14

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 allows both the 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.

Configuration Example

#Set the transformation set mode to tunnel mode.

```

FS(config)#
FS(config)#crypto ipsec transform-set myset
FS(cfg-crypto-trans)#mode tunnel
FS(cfg-crypto-trans)#mode transport
FS(cfg-crypto-trans)#
```

Verification

N/A

9.39 reverse-route

Use this command to enable the reverse route injection function. When this command is configured, the IPSec module automatically adds a static route destined for the peer end of a tunnel or a specified IP address after the negotiation of the tunnel is completed.

reverse-route [**remote-peer** *ip-address*] [***distance***]

Use the **no** form of this command to disable the reverse route injection function.

no reverse-route [**remote-peer** *ip-address*] [***distance***]

Parameter Description

Parameter	Description
ip-address	(Optional) Specifies the next-hop address.
distance	Specifies the next-hop distance. The value range is from 1 to 255.

Defaults The reverse route injection function is disabled by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide You can run the **show ip route** command to display added routes.

You can run the **debug crypto IPSec** command to display information about added routes and deleted routes.

Configuration Example #Enable the reverse route injection function in the mapping encryption entry named mymap.

```
FS(config)# crypto map mymap 5 ipsec-isakmp
FS(config-crypto-map)# reverse-route
```

Verification N/A

9.40 self-identity

Use this command to specify the form of the local identity.

self-identity { **address** | **fqdn** *fqdn* | **user-fqdn** *user-fqdn* }

Use the **no** form of this command to restore the default local identity form.

no self-identity

Parameter Description

Parameter	Description
address	Indicates the local IP address.

fqdn	Indicates the local domain name.
user-fqdn	Indicates the local username and domain name.

Defaults The local identity uses the local IP address by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to set the identity for the negotiation initiated in aggressive mode. You can use the domain name or address to specify the local identity.

Configuration Example #Set the local identity.

```
FS(config)# self-identity fqdn www.vpdn.com
FS(config)# self-identity address
```

Verification N/A

9.41 set autoup

Use this command to set tunnel auto-connection.

set autoup

Use the **no** form of this command to restore the default configuration.

no set autoup

Parameter Description

Parameter	Description
access-list-number	Indicates the ACL No. (100-199, 2000-2699, and 2900-3899). Encryption mapping entries use only IP extended ACLs.

Defaults Tunnel auto-connection is disabled by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide Use this command to prevent packet loss caused by tunnel negotiation. Use this function in scenarios where data transmission is sensitive to tunnels and the tunnels need to be in the Up state at any time.

Configuration Example #Set the tunnel auto-connection.

```
FS(config)# crypto map mymap 10 IPSec-isakmp
FS(config-crypto-map)# set autoup
```

Verification N/A

9.42 set exchange-mode

Use this command to set the work mode used in Phase 1 of IKE negotiation between peers.

set exchange-mode { **main** | **aggressive** }

Use the **no** form of this command to restore the default work mode.

no set exchange-mode

Parameter Description

Parameter	Description
main	Indicates the main mode.
aggressive	Indicates the aggressive mode.

Defaults The main mode is used by default.

Command Mode Encryption mapping configuration mode

Default Level 14

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 aggressive 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 aggressive mode is recommended.

Configuration Example #Set the work mode to aggressive mode.

```
FS(config)# crypto map mymap 10 IPSec-isakmp
FS(config-crypto-map)# set exchange-mode aggressive
```

Verification N/A

9.43 set isakmp-policy

Use this command to specify a policy for negotiating a mapping set.

set isakmp-policy *number*

Use the **no** form of this command to cancel a policy for negotiation.

no set isakmp-policy

Parameter Description

Parameter	Description
number	Indicates the serial number of the specified policy for negotiation.

Defaults No policy is specified for negotiation by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide In aggressive mode, the device in the branch sends the policy of the highest priority to the device in the headquarters for negotiation by default. Therefore, if the same device in the branch negotiates with multiple devices in the headquarters in aggressive mode, the policy of the highest priority on each device in the headquarters needs to be consistent with that on the device in the branch, which reduces device compatibility. Use this command to specify a policy for negotiating a mapping set. In this way, the policy of the highest priority on each device in the headquarters does not need to be consistent with that on the device in the branch. This command is effective only to static mapping sets and is unavailable to dynamic mapping sets.

Configuration Example #Specify the policy with the serial number 2 for negotiation in the static mapping set named FS.

```
11.x_site1(config)#crypto map FS 100 ipsec-isakmp
11.x_site1(config-crypto-map)#set isakmp-policy 2
```

Verification N/A

9.44 set local (IPSec)

Use this command to specify the local IP address in an encryption mapping entry.

set local *ip-address*

Use the **no** form of this command to delete the local peer from an encryption mapping entry.

no set local *ip-address*

Parameter Description

Parameter	Description
ip-address	Indicates the local IP address.

Defaults No local peer is specified by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide

Use this command to set the local IP address used in the negotiation. The main address of the interface is used for negotiation when the IP address is not configured. The specified IP address is used for negotiation after configuration.

Configuration Example

#Specify a local peer (2.2.2.2) in the mapping encryption entry named mymap.

```
FS(config)# crypto map mymap 5 IPSec-isakmp
FS(config-crypto-map)# set local 2.2.2.2
```

Verification

N/A

9.45 set mtu

Use this command to set the IPSec pre-fragmentation mode (valid in tunnel mode).

set mtu *length*

Use the **no** form of this command to disable the IPSec pre-fragmentation mode.

no set mtu

Parameter Description

Parameter	Description
length	Indicates the size of a data packet fragment prior to encapsulation. The value range is from 512 to 1,500.

Defaults

The IPSec pre-fragmentation mode is disabled by default.

Command Mode

Encryption mapping configuration mode

Default Level

14

Usage Guide

Specify the pre-fragmentation mode for IPSec tunnel encapsulation.

Configuration Example

#Specify the pre-fragmentation mode in the encryption mapping set named mymap.

```
FS(config)# crypto map mymap 5 IPSec-isakmp
FS(config-crypto-map)# set mtu 1000
```

Verification

N/A

9.46 set peer (IPSec)

Use this command to specify a remote peer in an encryption mapping entry.

set peer { *hostname* | *ip-address* }

Use the **no** form of this command to delete the remote peer from an encryption mapping entry.

no set peer { *hostname* | *ip-address* }

Parameter Description

Parameter	Description
ip-address	Indicates the IP address of the remote peer.
hostname	Indicates the host name of the remote peer.

Defaults No remote peer is specified by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide A remote peer must be specified for an encryption mapping entry in use.

When there are multiple certificate chains locally, specify the certificate chain according to each peer. If no local certificate chain is specified, the peer certificate chain (CA certificate) is used for authentication. When the peer certificate chain is not specified, the default certificate chain (CA certificate) is used for authentication.

Configuration Example #Specify a remote peer (2.2.2.2) in the mapping encryption entry named mymap.

```
FS(config)# crypto map mymap 5 IPSec-isakmp
FS(config-crypto-map)# set peer 2.2.2.2
```

Verification N/A

9.47 set peer-identical

Use this command to specify multiple ACEs to use the same remote peer in the negotiation in Phase 2.

set peer-identical

Use the **no** form of this command to delete the same remote peer configured in multiple ACEs used in the negotiation in Phase 2.

no set peer-identical

Parameter Description

Parameter	Description
N/A	N/A

Defaults No identical remote peer is specified for multiple ACEs in the negotiation in Phase 2 by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide When multiple ACEs are configured in an ACL and multiple remote peers are configured, use this command to ensure that all ACEs use the same peer for negotiation.

Configuration Example #Specify ACEs to use the same remote peer in the encryption mapping entry named mymap.

```
FS(config)# crypto map mymap 5 IPSec-isakmp
FS(config-crypto-map)# set peer-identical
```

Verification N/A

9.48 set peer-preempt

Use this command to specify the remote peer of a higher priority to initiate preemption.

set peer-preempt

Use the **no** form of this command cancel the configuration of requesting the remote peer of a higher priority to initiate preemption.

no set peer-preempt

Parameter Description

Parameter	Description
N/A	N/A

Defaults No remote peer of a higher priority is specified to initiate preemption by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide Use the peer of a higher priority for negotiation when multiple remote peers are configured.

Multiple remote peers can be configured for one encryption mapping set. A remote peer configured earlier has a priority higher than that of a remote peer configured later. The peer of a higher priority is used for negotiation. When the device switches to another peer for negotiation after a tunnel is interrupted, if the peer of a higher priority can initiate negotiation, the peer of the higher priority is used for negotiation and forwarding and the tunnel negotiation using the peer of a lower priority is interrupted. This command must be configured to implement the preceding functions.

Configuration Example #Specify the remote peer of a higher priority to initiate preemption in the encryption mapping set named mymap.

```
FS(config)# crypto map mymap 5 IPSec-isakmp
FS(config-crypto-map)# set peer-preempt
```

Verification N/A

9.49 set pfs (IPSec)

Use this command to specify the Diffie-Hellman group ID used in IPSec tunnel encapsulation.

set pfs { **group1 | group2** }

Use the **no** form of this command to cancel the Diffie-Hellman group ID used in tunnel encapsulation.

no set pfs

Parameter Description

Parameter	Description
group1	Indicates the 768-bit group.
group2	Indicates the 1024-bit group.

Defaults

No Diffie-Hellman group is used by default.

Command Mode

Encryption mapping configuration mode

Default Level

14

Usage Guide

Specify the Diffie-Hellman group ID used in IPSec tunnel encapsulation.

Configuration Example

#Specify the 1024-bit Diffie-Hellman group in the encryption mapping set named mymap.

```
FS(config)# crypto map mymap 5 IPSec-isakmp
FS(config-crypto-map)# set pfs group2
```

Verification

N/A

9.50 set security-association lifetime

Use this command to set the global lifetime used for IPSec SA association in an encryption mapping set.

set security-association lifetime { **seconds** *seconds* | **kilobytes** *kilobytes*] }

Use the **no** form of this command to restore the default value of global lifetime used for IPSec SA association in an encryption mapping set.

no set security-association lifetime { **seconds** | **kilobytes** }

Parameter Description

Parameter	Description
seconds *seconds*	Indicates the SA timeout period in seconds. The value range is from 120 to 86400.
kilobytes *kilobytes*	Indicates the timeout communication amount of an SA in kilobytes. The value range is from 2,560 to 536,870,912.

Defaults

SAs in an encryption mapping set are negotiated based on the global lifetime.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide This command is effective only to encryption mapping entries used for negotiation of IPSec SAs established via IKE and is unavailable to encryption mapping entries of SAs that are manually configured.

By default, all IPSec SAs are negotiated based on the global lifetime. If a different lifetime is required for SA negotiation for a specific destination IP address, use this command to change the lifetime in the encryption mapping entry that uses this destination address for negotiation.

ℹ This command changes the lifetime for IPSec SA negotiation in a specific encryption entry and does not affect the global lifetime.

Configuration Example #Change the lifetime of Entry 5 to 2,500 seconds in the encryption mapping set named mymap.

```
FS(config)# crypto map mymap 5 IPSec-isakmp
FS(config-crypto-map)# set security-association lifetime seconds 2500
```

Verification N/A

9.51 set session-key

Use this command to set the SPIs and passwords for relevant algorithms for inbound and outbound protected communication.

set session-key { **inbound | outbound** } **ah** *spi hex-key-data*

set session-key { **inbound | outbound** } **esp** *spi* { **cipher** *hex-key-data* **| authenticator** *hex-key-data* }

Use the **no** form of this command to delete the SPIs and passwords of relevant algorithms.

no set session-key { **inbound** | **outbound** } **ah**

no set session-key { **inbound | outbound** } **esp**

Parameter Description

Parameter	Description
Spi	Indicates the SPI.
hex-key-data	Indicates a password in hexadecimal notation.

Defaults No SPI or password of any algorithm is specified by default.

Command Mode Encryption mapping configuration mode

Default Level 14

Usage Guide This command is applicable only to manually configured SAs and is used only in **IPSec-manual**.

Configuration Example

#Specify the ESP encapsulation in the encryption mapping set named mymap and set the encapsulation and decapsulation passwords to abcdef1234567890.

```
FS(config)# crypto map mymap 5 ipsec-manual
FS(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890
FS(config-crypto-map)# set session-key outbound esp 300 cipher abcdef1234567890
```

Verification

N/A

9.52 set transform-set

Use this command to specify transformation sets to be used in an encryption mapping entry.

Set transform-set *transform-set-name1* [*transform-set-name2*] [*transform-set-name3*] [*transform-set-name4*] [*transform-set-name5*] [*transform-set-name6*]

Use the **no** form of this command to delete all transformation sets from an encryption mapping entry.

no set pfs

Parameter Description

Parameter	Description
transform-set-name1, *[transform-set-name2],* *[transform-set-name3],* *[transform-set-name4],* *[transform-set-name5],* *[transform-set-name6]*	Indicates the name of a transformation set. A maximum of six transformation sets can be specified in one encryption mapping entry.

Defaults

No transformation set is specified by default.

Command Mode

Encryption mapping configuration mode

Default Level

14

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.

Configuration Example

#Specify the transformation set named myset in the encryption mapping entry.

```
FS(config)# crypto IPSec transform-set myset esp-des esp-sha-hmac
FS(config)# crypto map mymap 5 IPSec-isakmp
FS(config-crypto-map)# set transform-set myset
```

Verification

N/A

9.53 show crypto dynamic-map (IPSec)

Use this command to display dynamic encryption mapping information.

show crypto dynamic-map [*map-name*]

Parameter Description

Parameter	Description
map-name	Indicates the name of an encryption mapping set.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

Use this command to display the PIM interfaces on the device, PIM neighbors of interfaces, Hello message retransmission interval, DR address, and other information.

Configuration Example

#Display information about all dynamic encryption mapping sets.

```
FS# show crypto dynamic-map
            Crypto Map Template "mydmap" 1
No matching address list set.
Security association lifetime: 4608000 kilobytes/3600 seconds(id=34)
PFS (Y/N): N
Transform sets = {    }
```

9.54 show crypto IPSec sa

Use this command to display information about the current active IPSec SA.

show crypto IPSec sa

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Display information about the current active IPSec SA.

```
Interface: GigabitEthernet 1/0/0
             Crypto map tag:mymap, local addr 2.2.2.3
             media mtu 1500
```

```
sub_map type:static, seqno:7, id=0
local    ident (addr/mask/prot/port): (2.2.2.3/0.0.0.0/0/0))
remote    ident (addr/mask/prot/port): (2.2.2.2/0.0.0.0/0/0))
PERMIT
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#send errors 0, #recv errors 0
Inbound esp sas:
     spi:0x79b8e4bb (2042160315)
      transform: esp-3des
      in use settings={Tunnel,}
      crypto map mymap 7
      sa timing: remaining key lifetime (k/sec): (4607000/3505)
      IV size: 8 bytes
      max reply windows size: 0
      Replay detection support:Y


Outbound esp sas:
     spi:0x293b8b55 (691768149)
      transform: esp-3des
      in use settings={Tunnel,}
      crypto map mymap 7
      sa timing: remaining key lifetime (k/sec): (4607000/3505)
      IV size: 8 bytes
      max reply windows size: 0
      Replay detection support:Y
```

9.55 show crypto IPSec transform-set

Use this command to display information about transformation sets configured for the device.

show crypto IPSec transform-set

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Display information about transformation sets configured for the device.

```
FS# show crypto IPSec transform-set
transform set myset3: { esp-des,}
        will negotiate = {Tunnel,}
```

9.56 show crypto isakmp policy

Use this command to display the IKE policy configured for the device.

show crypto isakmp policy

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Display the IKE policy configured for the device.

```
FS# show crypto isakmp policy
Protection suite of priority 9
encryption algorithm:     3DES - Data Encryption Standard (56 bit keys).
hash algorithm:            Message Digest 5
authentication method:    Pre-Shared Key
Diffie-Hellman group:     #2 (1024 bit)
lifetime:                  1000 seconds
Protection suite of priority 10
encryption algorithm:     DES - Data Encryption Standard (56 bit keys).
hash algorithm:            Message Digest 5
authentication method:    Pre-Shared Key
Diffie-Hellman group:     #2 (1024 bit)
lifetime:                  1000 seconds
Default protection suite
encryption algorithm:     DES - Data Encryption Standard (56 bit keys).
hash algorithm:            Secure Hash Standard
authentication method:    Pre-Shared Key
Diffie-Hellman group:     #1 (768 bit)
lifetime:                  86400seconds
```

9.57 show crypto isakmp sa

Use this command to display the current active IKE SA on the device.

show crypto isakmp sa

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Example #Display the current active IKE SA on the device.

```
FS# show crypto isakmp sa
destination    source     state      conn-id    lifetime(second)
  1.1.1.1        1.1.1.2    IKE_IDLE   59           32254
```

9.58 show crypto log

Use this command to display IPSec VPN login and logout logs.

show crypto log

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Example #Display IPSec VPN login and logout logs.

```
FS # sh cr log
Time                        RemoteName                                                      PeerIP/Port
Action            Reason            Interface                 Proto:(Local)ip/mask/port <--> (Peer)ip/mask/port


--------------------     ------------------------------------------------------------     ---------------------------------------------     ---------------
--------------- ----------------------     ----------------------------------------------------------------------------------------------------------------
2014-11-15-01:07:06     3.3.3.3                                                         3.3.3.3/500
logout            DEL_IPS_PKT       Gi0/1                     17:3.3.3.3/32/1701<-->3.3.3.3/32/1701
2014-11-15-01:07:06     3.3.3.3                                                         3.3.3.3/500
```

```
logout          DEL_ISA_PKT      Gi0/1                    NULL
```

9.59 show crypto log remotename

Use this command to display IPSec VPN login and logout logs that are filtered by peer name (or IP address).

show crypto log remotename *name*

Parameter Description

Parameter	Description
name	Specifies the peer name used for filtering and displaying logs.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Display IPSec VPN login and logout logs that are filtered by peer name (or IP address).

```
11.x_site1#show crypto log remotename 61.100.1.20

total log numbers: 184


Time                        RemoteName                                                            PeerIP/Port
Action          Reason          Interface               Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

--------------------    ------------------------------------------------------------    ---------------------------------------------    ----------------
---------------- ----------------------    -----------------------------------------------
2015-10-16-03:50:14     61.100.1.20                                                              61.100.1.20/500
login           NA               Gi0/2                    NULL
2015-10-16-03:50:14     61.100.1.20                                                              61.100.1.20/500
login           NA               Gi0/2                    0:1.1.1.0/24/0<-->2.2.2.0/24/0
2015-10-16-03:55:50     61.100.1.20                                                              61.100.1.20/500
logout          CLR_ISA_SA       Gi0/2                    0:1.1.1.0/24/0<-->2.2.2.0/24/0
2015-10-16-03:56:51     61.100.1.20                                                              61.100.1.20/500
logout          IDLE_TIMER       Gi0/2                    NULL
Filter log numbers: 4
11.x_site1#
```

9.60 show crypto log remotename name start start_lines end end_lines

Use this command to display IPSec VPN login and logout logs that are filtered by peer name (or IP address) and are in specified lines.

show crypto log remotename *name* **start** *start_lines* **end** *end_lines*

Parameter Description

Parameter	Description
name	Specifies the peer name used for filtering and displaying logs.
start_lines	Specifies the start line of logs to be displayed.
end_lines	Specifies the end line of logs to be displayed.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Example #Display IPSec VPN login and logout logs that are filtered by peer name (or IP address) and are in specified lines.

```
11.x_site1#show crypto log remotename 61.100.1.20 start 1 end 2

total log numbers: 188


Time                    RemoteName                                                          PeerIP/Port
Action          Reason          Interface               Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

-------------------     -------------------------------------------------------     -----------------------------------------     ---------------
--------------- ---------------------     -------------------------------------------
2015-10-16-03:50:14     61.100.1.20                                                      61.100.1.20/500
login           NA              Gi0/2                   NULL
2015-10-16-03:50:14     61.100.1.20                                                      61.100.1.20/500
login           NA              Gi0/2                   0:1.1.1.0/24/0<-->2.2.2.0/24/0
Filter log numbers: 4
```

9.61 show crypto log start start_lines end end_lines

Use this command to display IPSec VPN login and logout logs in specified lines.

show crypto log start *start_lines* **end** *end_lines*

Parameter Description

Parameter	Description
start_lines	Specifies the start line of logs to be displayed.
end_lines	Specifies the end line of logs to be displayed.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Example

#Display IPSec VPN login and logout logs in specified lines.

```
11.x_site1#show crypto log start 1 end 2

total log numbers: 184


Time                          RemoteName                                                         PeerIP/Port
Action              Reason               Interface                    Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

--------------------    ------------------------------------------------------------    --------------------------------------------    ---------------
--------------- ----------------------    ----------------------------------------------
2015-10-16-03:23:55        NO_NAME                                                                        (null)/0
restart             IPSEC_RESTART                                     NULL
2015-10-16-03:42:57        NO_NAME                                                                        (null)/0
restart             IPSEC_RESTART                                     NULL
11.x_site1#
```

9.62 show crypto map (IPSec)

Use this command to display information about an encryption mapping set.

show crypto map [*map-name*]

Parameter Description

Parameter	Description
map-name	Indicates the name of an encryption mapping set.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Example

#Display information about all encryption mapping sets.

```
FS# show crypto map

Crypto Map:"mymap1" 1 IPSec-isakmp, (Complete)
            Extended IP access list 100
            Security association lifetime: 0 kilobytes/120 seconds(id=2)
```

```
        PFS (Y/N): N
        Transform sets = { myset3,   }

        Interfaces using crypto map mymap1:
                GigabitEthernet 1/1/0
```

9.63 tunnel protection IPSec profile

Use this command to apply a defined encryption mapping set (profile) to a tunnel interface.

tunnel protection IPSec profile [*profile-name*]

Use the **no** form of this command to cancel the association between an interface and an encryption mapping set.

no tunnel protection IPSec profile [*profile-name*]

Parameter Description

Parameter	**Description**
profile-name	Indicates the name of an encryption mapping set (profile).

Defaults

No encryption mapping set is applied to a tunnel interface by default.

Command Mode

Interface configuration mode

Default Level

14

Usage Guide

Use this command to apply an encryption mapping set to an interface. An encryption mapping set must be applied to a tunnel interface so that IPSec encryption and protection can be provided for all packets of the tunnel interface. One interface can be associated with only one encryption mapping set.

Encryption mapping sets (profiles) can be applied only to tunnels that support GRE, or IPIP. If they are configured on an unsupported tunnel or the tunnel mode is changed to a mode that is not supported by the encryption mapping sets (profiles), the encryption mapping sets configured on the tunnel interfaces will be deleted.

Configuration Example

1. #Apply the encryption mapping set named profile-name to Interface Tunnel 1.

```
FS(config)# interface tunnel 1
FS(config-if-Tunnel 1) # tunnel protection IPSec profile profile-name
```

2. #Apply the encryption mapping set named test to Interface virtual-ppp 1.

```
FS(config)#crypto ipsec profile test
FS(config-crypto-profile)#exit
FS(config)#
FS(config)#int virtual-ppp 1
FS(config-if-Virtual-ppp 1)#tunnel protection ipsec profile test
FS(config-if-Virtual-ppp 1)#exit
FS(config)#
```

Verification	N/A

10 ITBOX Commands

10.1 evpn-server clear-remark

Use this command to clear remarks information of a specified branch

evpn-server clear-remark sn *sn*

Parameter Description

Parameter	Description
sn	Serial number of the branch

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear remarks information of a specified branch.

Configuration Example

#Clear remarks information of a specified branch.

```
FS# evpn-server clear-remark sn G1HD927000001
```

Verification

Run the **show evpn-server client** command to check whether the branch information is restored.

10.2 evpn-server delete

Use this command to delete a specified branch.

evpn-server delete sn *sn*

Parameter Description

Parameter	Description
sn	Serial number of the branch

Command Mode

Privileged EXEC mode

Usage Guide

After a branch is deleted, the headquarters do not manage the branch and cannot display information about the branch.

Configuration Example

#Delete a branch.

```
FS# evpn-server delete sn G1HD927000001
```

Verification

Verify that no information is displayed after the **show evpn-server client** command is run.

10.3 evpn-server outside-ip

Use this command to configure the public IP address and Web access port of the local device.

evpn-server outside-ip *A.B.C.D* **web-port** *port-value*

Use the **no** form of this command to delete the configured public IP address and Web access port of the local device.

no evpn-server outside-ip

Parameter Description

Parameter	**Description**
A.B.C.D	Public IP address
port-value	ID of the Web access port

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command only records information and is used to generate branch configurations. It cannot change the IP address or Web access port of the device.

The public IP address is the server address filled in when a VPN is configured for the branch.

Configuration Example

#Configure the public IP address of a device as 3.3.3.3 and the ID of the Web access port as 8000.

```
FS(config)# evpn-server outside 3.3.3.3 web 8000
```

Verification

Run the **show evpn-server config** command to display the configuration information.

```
FS# show evpn config
port-mask         : 001100
server-ip         : 3.3.3.3
server-port       : 8000
```

10.4 evpn-server port-mask

Use this command to configure a branch LAN port that needs to be monitored.

evpn-server port-mask *mask-value*

Use the **no** form of this command to clear a monitored LAN port.

no evpn-server port-mask

Parameter Description

Parameter	**Description**
mask-value	LAN port mask, which is a binary number. The second port form the right is Port 1 and the third port from the right is Port 2, and the rest can be deduced by analogy.

Defaults

N/A

Command

Global configuration mode

Mode

Usage Guide After the port that needs to be monitored is configured, a branch with the specified monitored port being abnormal is displayed when you query branches with abnormal ports.

Configuration Example

1. #Monitor LAN Port 1.

```
FS(config)# evpn-server port-mask 100
```

2. # Monitor LAN Ports 3 and 4.

```
FS(config)# evpn-server port-mask 110000
```

Verification

1. Run the **show evpn-server config** command to display the configuration status.

```
FS#show evpn config
port-mask         : 110000
server-ip         : 3.3.3.3
server-port       : 8000
```

2. Run the **show evpn-server client port-off** command to check whether the displayed branch is a branch of which not all monitored ports are in the UP state.

10.5 evpn-server reload

Use this command to restart the device of a specified branch.

evpn-server reload sn *sn*

Parameter Description

Parameter	Description
sn	Serial number of the branch

Command Mode Privileged EXEC mode

Usage Guide Use this command to restart the device of the branch when an exception occurs.

Configuration Example

#Restart the device of a branch.

```
FS# evpn-server reload sn G1HD927000001
```

Verification Run the **evpn-server shell** command to display the power-on time of the device of the specified branch.

10.6 evpn-server remark

Use this command to add remarks information for a specified branch.

evpn-server remark sn sn [**name** name] [**manager** manager] [**phone** phone]

Use this command to add address remarks for a specified branch.

evpn-server remark sn sn [**province** province] [**city** city] [**district** district]

Parameter Description

Parameter	Description
sn	Serial number of the branch
name	Branch name
manager	Branch administrator
phone	Contact Tel. No.
province	Province where the branch is located
city	City where the branch is located
district	District where the branch is located

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Example #Add remarks for a branch administrator.

```
FS# evpn-server remark sn G1HD927000001 manager Zhang San
```

Verification Run the **show evpn-server client** command to check whether remarks are added for a branch.

10.7 evpn-server reset

Use this command to reconnect the device in the headquarters with the device in a specified branch.

evpn-server reset sn *sn*

Parameter Description

Parameter	Description
sn	Serial number of the branch

Command Mode Privileged EXEC mode

Usage Guide Use this command to re-establish a connection, so that the device in the headquarters can deliver configurations to the device in a branch.

Configuration Example # Reset the connection with the device in a branch.

```
evpn-server reset sn G1HD927000001
```

Verification N/A

10.8 evpn-server shell

Use this command to deliver a shell script to all online branch devices.

evpn-server shell *all-clients* { **string** *scripts* | **file** *path* }

Use this command to deliver a shell script to the device of a specified branch.

evpn-server shell sn *sn* { **string** *scripts* | **file** *path* } [**with-result**]

Parameter Description

Parameter	Description
sn	Serial number of the branch
scripts	Script string
path	Script file path

Command Mode

Privileged EXEC mode

Usage Guide

Use the key word **with-result** to display the script running result.

Configuration Example

1. #Display power-on time of the device of a branch.

```
FS# evpn-server shell sn G1HD927000001 string "uptime" with-result
```

2. #Deliver VPN configurations to all branch devices.

```
FS# evpn-server shell all-clients file "/data/evpn/cfg_vpn.sh.text"
```

10.9 evpn-server version

Use this command to upgrade the device of a branch to a specified system version.

evpn-server version *product version*

Use the **no** form of this command to stop upgrading the device of the branch.

no evpn-server version *product*

Parameter Description

Parameter	Description
product	Product name
version	System version number

Defaults

The device of a branch is not upgraded by default.

Command Mode

Global configuration mode

Usage Guide

Before configuration, rename the upgrade package as **iTBox.tgz** and place the upgrade package to the

/mnt/sata0/evpn sub directory.

Configuration Example

#Upgrade the branch system of FS-MA1210 to the version 1.0.0.1114.

```
FS(config)# evpn-server version FS-MA1210 1.0.0.1114
```

Verification

After the device of a branch is upgraded, run the **evpn-server shell** command to check the system version number of the device.

```
FS# evpn-server shell sn G1HD927000001 string “cat /proc/fs_sys/software_version” with-result
1.0.0.1114FS#
```

10.10 show evpn-server client

Use this command to display status statistics of a branch device.

show evpn-server client info

Use this command to display branches that request for access.

show evpn-server client new

Use this command to display branches with the device being offline

show evpn-server client offline [**province** *province*] [**city** *city*] [**district** *district*]

Use this command to display branches with the device being online

show evpn-server client online [**province** *province*] [**city** *city*] [**district** *district*]

Use this command to display branches with a port exception.

show evpn-server client port-off [**province** *province*] [**city** *city*] [**district** *district*]

Use this command to display a specified branch.

show evpn-server client sn *sn*

Use this command to display branches with a VPN exception.

show evpn-server client vpn-off [**province** *province*] [**city** *city*] [**district** *district*]

Use this command to display branches with a normal VPN.

show evpn-server client vpn-on [**province** *province*] [**city** *city*] [**district** *district*]

Parameter Description

Parameter	Description
province	Province
city	City
district	District
sn	Serial number of the branch

Command

Global configuration mode and privileged EXEC mode

Mode

Usage Guide The results of some commands can be filtered by province, city, and district.

Configuration Example 1. #Display status statistics of a branch device.

```
FS#show evpn-server client info
online      : 2
offline     : 1
vpn_on      : 2
vpn_off     : 0
port_off    : 2
```

2. #Display branches with a normal VPN.

```
FS#show evpn client vpn-on
sn                    name                                                                                    manager
phone                 port                province          city                          district
---------------    ----------------------------------------------------------------    ---------------    ---------------    ---------------    ---------------
------------------------- ---------------------------
G1HD927000001       Cangshan Shop                                                                               Zhang
San                     13012345678            000000                      Fujian                               Fuzhou
Cangshan
```

10.11 show evpn-server config

Use this command to display current configurations.

show evpn-server config

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Global configuration mode and privileged EXEC mode

Usage Guide N/A

Configuration Example #Display current configurations

```
FS# show evpn-server config
port-mask         : 000100
server-ip         : 3.3.3.3
server-port       : 8000
```

11 AAA Commands

11.1 aaa accounting commands

Use this command to configure NAS command accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting commands *level* **{ default |** *list-name* **} start-stop** *method1* [*method2*…]

no aaa accounting commands *level* { **default |** *list-name* }

Parameter Description

Parameter	Description
level	The accounting command level, 0-15. The message shall be recorded before which command level is executed is determined.
default	When this parameter is used, the following defined method list is used as the default method for command accounting.
list-name	Name of the command accounting method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
none	Does not perform accounting.
group	Uses the server group for accounting, the TACACS+ server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

FSOS enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service.

The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Configuration Examples

The following example enables NAS command accounting.

```
FS(config)# aaa accounting commands 15 default start-stop group tacacs+
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication	Defines AAA authentication.
accounting commands	Applies the accounting commands to the terminal line.

Platform Description

N/A

11.2 aaa accounting exec

Use this command to enable NAS access accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting exec { **default |** *list-name* } **start-stop** *method1* [*method2…*]

no aaa accounting exec { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec accounting.
list-name	Name of the Exec accounting method list, which could be any character strings
method	It must be one of the keywords: **none** and **group**. One method list can contain up to four methods.
none	Does not perform accounting.
group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide FSOS enables the exec accounting function after enabling the login authentication.

After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user logs in, it does not send the account stop information to the security server when a user logs out, either.

The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Configuration Examples The following example enables NAS access accounting.

```
FS(config)# aaa accounting network start-stop group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication	Defines AAA authentication.
accounting commands	Applies the Exec accounting to the terminal line.

Platform Description N/A

11.3 aaa accounting network

Use this command to enable network access accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting network { default | *list-name* **} start-stop** *method1* [*method2*..]

no aaa accounting network { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Network accounting.
list-name	Name of the accounting method list
method	Sends accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
none	Does not perform accounting.
group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

FSOS performs accounting of user activities by sending record attributes to the security server. Use the **start-stop** keyword to set the user accounting option.

Configuration Examples

The following example enables network access accounting.

```
FS(config)# aaa accounting network start-stop group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization network	Defines a network authorization method list.
aaa authentication	Defines AAA authentication.
username	Defines a local user database.

Platform Description

N/A

11.4 aaa accounting update

Use this command to enable the accounting update function.

Use the **no** form of this command to restore the default setting.

aaa accounting update

no aaa accounting update

Parameter Description

N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration Examples

The following example enables the accounting update function.

```
FS(config)# aaa new-model
FS(config)# aaa accounting update
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform Description

N/A

11.5 aaa accounting update periodic

Use this command to set the interval of sending the accounting update message.

Use the **no** form of this command to restore the default setting.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter Description

Parameter	Description
interval	Interval of sending the accounting update message, in the unit of minutes. The shortest interval is 1 minute.

Defaults

The default is 5 minutes.

Command Mode

Global configuration mode

Usage Guide

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration Examples

The following example sets the interval of accounting update to 1 minute.

```
FS(config)# aaa new-model
FS(config)# aaa accounting update
FS(config)# aaa accounting update periodic 1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform Description

N/A

11.6 aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list.

Use the **no** form of this command to delete the user authentication method list.

aaa authentication enable default *method1* [*method2*...]

no aaa authentication enable default

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
method	It must be one of the keywords: **local, none** and **group**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
enable	Enables AAA Enable authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable authentication negotiation. You must use the **aaa authentication enable** command to configure a default or optional method list for Enable authentication.

The next method can be used for authentication only when the current method does not work.

The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

Configuration Examples

The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
FS(config)# aaa authentication enable default group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
enable	Switchover the user level.
username	Defines a local user database.

Platform Description

N/A

11.7 aaa authentication iportal

Use this command to enable AAA Portal Web user authentication.

Use the **no** form of this command to delete the authentication method list.

aaa authentication iportal { **default** | *list-name* } *method1* [*method2*...]

no aaa authentication iportal { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
list-name	Name of the user authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none**, **subs** and **group**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA Portal Web security service is enabled on the device, users must use AAA for Portal Web authentication negotiation. You must use the **aaa authentication iportal** command to configure a default or optional method list for Portal Web authentication.

Configuration Examples

The following example defines an AAA Portal Web authentication method list named **rds_web**. First the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
FS(config)# aaa authentication iportal rds_web group radius local
```

Related

Command	Description

Commands

aaa new-model	Enables the AAA security service.
login authentication	Applies the Login authentication method to the terminal lines.
username	Defines a local user database.

Platform Description

N/A

11.8 aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list.

Use the **no** form of this command to delete the authentication method list.

aaa authentication login { **default** | *list-name* } *method1* [*method2*..]

no aaa authentication login { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
list-name	Name of the user authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none**, **group** and **subs**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
subs	Uses the subs database for authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use the **aaa authentication login** command to configure a default or optional method list for Login authentication.

The next method can be used for authentication only when the current method does not work.

You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

Configuration Examples

The following example defines an AAA Login authentication method list named list-1. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
FS(config)# aaa authentication login list-1 group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
login authentication	Applies the Login authentication method to the terminal lines.
username	Defines a local user database.

Platform Description

N/A

11.9 aaa authentication ppp

Use this command to enable the AAA authentication for PPP user and configure the PPP user authentication method list.

Use the **no** form of this command to delete the authentication method list.

aaa authentication ppp { **default** | *list-name* } *method1* [*method2*...]

no aaa authentication ppp { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication.
list-name	Name of the user authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none group** and **subs**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA PPP security service is enabled on the device, users must use AAA authentication for PPP negotiation. You must use the **aaa authentication ppp** command to configure a default or optional method list for PPP user authentication.

The next method can be used for authentication only when the current method does not work.

Configuration Examples

The following example defines an AAA authentication method list named rds_ppp for PPP session. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
FS(config)# aaa authentication ppp rds_ppp group radius local
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
ppp authentication	Associates a specific method list with the PPP user.
username	Defines a local user database.

Platform Description

N/A

11.10 aaa authentication sslvpn

Use this command to enable AAA authentication for the SSL VPN user and configure the SSL VPN user authentication method list.

Use the **no** form of this command to delete the authentication method list.

aaa authentication sslvpn { **default** | *list-name* } *method1* [*method2*...]

no aaa authentication sslvpn { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for SSL VPN user authentication.
list-name	Name of SSL VPN user authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none**, **subs** and **group**. One method list can contain up to four methods.
local	Use the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the SSL VPN security service is enabled on the device, users must use the AAA authentication for SSL VPN negotiation. You must use the **aaa authentication sslvpn** command to configure a default or optional method list for user authentication.

The next method can be used for authentication only when the current method does not work.

Configuration Examples

The following example defines an AAA authentication method list named **rds_sslvpn** for SSL VPN session. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
FS(config)# aaa authentication sslvpn rds_sslvpn group radius local
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

11.11 aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI. Use the **no** form of this command to restore the default setting.

aaa authorization commands *level* { **default** | *list-name* } *method1* [*method2*...]

no aaa authorization commands *level* { **default** | *list-name* }

Parameter Description

Parameter	Description
level	Command level to be authorized in the range from 0 to 15
default	When this parameter is used, the following defined method list is used as the default method for command authorization.
list-name	Name of the user authorization method list, which could be any character strings
method	It must be one of the keywords: **none** and **group**. One method list can contain up to four methods.
none	Do not perform authorization.
group	Uses the server group for authorization. At present, the TACACS+ server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

FSOS supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny.

It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level.

The configured command authorization method must be applied to terminal line which requires the command authorization. Otherwise, the configured command authorization method is ineffective.

Configuration Examples

The following example uses the TACACS+ server to authorize the level 15 command.

```
FS(config)# aaa authorization commands 15 default group tacacs+
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
authorization commands	Applies the command authorization for the terminal line.

Platform Description

N/A

11.12 aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode).

Use the **no** form of this command to restore the default setting.

aaa authorization config-commands

no aaa authorization config-commands

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.

Configuration Examples

The following example enables the configuration command authorization function.

```
FS(config)# aaa authorization config-commands
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization commands	Defines the AAA command authorization.

Platform Description

N/A

11.13 aaa authorization console

Use this command to authorize the commands of the users who have logged in the console.

Use the **no** form of this command to restore the default setting.

aaa authorization console

no aaa authorization console

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

FSOS supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.

Configuration Examples

The following example enables the aaa authorization console function.

```
FS(config)# aaa authorization console
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization commands	Defines the AAA command authorization.
authorization commands	Applies the command authorization to the terminal line.

Platform Description

N/A

11.14 aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level.

Use the **no** form of this command to restore the default setting.

aaa authorization exec { **default** | *list-name* } *method1* [*method2*...]

no aaa authorization exec { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec authorization.
list-name	Name of the user authorization method list, which could be any character strings
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
local	Uses the local user name database for authorization.
none	Does not perform authorization.
group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

FSOS supports authorization of users logged in the NAS CLI and assignment of CLI authority level (0-15). The **aaa authorization exec** function is effective on condition that Login authentication function has been enabled. It cannot enter the CLI if it fails to enable the **aaa authorization exec**.

You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

Configuration Examples

The following example uses the RADIUS server to authorize Exec.

```
FS(config)# aaa authorization exec default group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
authorization exec	Applies the command authorization to the terminal line.
username	Defines a local user database.

Platform Description

N/A

11.15 aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network.

Use the **no** form of this command to restore the default setting.

aaa authorization network { **default** | *list-name* } *method1* [*method2*...]

no aaa authorization network { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Network authorization.
method	It must be one of the keywords: none and group. One method list can contain up to four methods.
none	Does not perform authorization.
group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

FSOS supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically.

Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used.

The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

Configuration Examples

The following example uses the RADIUS server to authorize network services.

```
FS(config)# aaa authorization network default group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting	Defines AAA accounting.
aaa authentication	Defines AAA authentication.
username	Defines a local user database.

Platform Description

N/A

11.16 aaa domain

Use this command to configure the domain attributes.

Use the **no** form of this command to restore the default setting.

aaa domain { **default** | *domain-name* }

no aaa domain { **default |** *domain-name* }

Parameter Description

Parameter	Description
default	Uses this parameter to configure the default domain.
domain-name	The name of the specified domain

Defaults

No domain is configured by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the domain-name–based AAA service. The **default** is to configure the default domain. That is the method list used by the network device if the users are without domain information. The *domain-name* is the specified domain name, if the users are with this *domain name*, the method lists associated with this domain are used. At present, the system can configure up to 32 domains.

Configuration Examples

The following example configures the domain name.

```
FS(config)# aaa domain FS.com
FS(config-aaa-domain)#
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description N/A

11.17 aaa domain enable

Use this command to enable domain-name-based AAA service.

Use the **no** form of this command to restore the default setting.

aaa domain enable

no aaa domain enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide To perform the domain-name-based AAA service configuration, enable this service.

Configuration Examples The following example enables the domain-name-based AAA service.

```
FS(config)# aaa domain enable
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
show aaa doamain	Displays the domain configuration.

Platform Description N/A

11.18 aaa local authentication attempts

Use this command to set login attempt times.

aaa local authentication attempts *max-attempts*

Parameter Description

Parameter	Description
max-attempts	In the range from 1 to 2,147,483,647

Defaults The default is 3.

Command Mode Global configuration mode

Usage Guide Use this command to configure login attempt times.

Configuration Examples

The following example sets login attempt times to 6.

```
FS #configure terminal
FS(config)#aaa local authentication attempts 6
```

Related Commands

Command	Description
show running-config	Displays the current configuration of the switch.
show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description

N/A

11.19 aaa local authentication lockout-time

Use this command to configure the lockout-time period when the login user has attempted for more than the limited times.

aaa local authentication lockout-time *lockout-time*

Parameter Description

Parameter	Description
lockout-time	In the range from 1 to 2,147,483,647 in the unit of minutes

Defaults

The default is 15 minutes.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times.

Configuration Examples

The following example sets the lockout-time period to 5 minutes.

```
FS#configure terminal
FS(config)#aaa local authentication lockout-time 5
```

Related Commands

Command	Description
show running-config	Displays the current configuration of the switch.
show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description

N/A

11.20 aaa local user allow public account

Use this command to allow the local account (username or subs) to be shared by multiple terminals with Web authentication configured or built-in.

aaa local user allow public account

Parameter Description

Parameter	Description
N/A	N/A

Defaults One local account cannot be shared by multiple terminals by default.

Command Mode Global configuration mode

Usage Guide This configuration is supported by EG series products only. For other products, a local account can be shared by multiple terminals by default.

Configuration Examples The following example allows the local account (username or subs) to be shared by multiple terminals with Web authentication configured or built-in.

```
FS#configure terminal
FS(config)#aaa local user allow public account
```

Related Commands

Command	Description
N/A	N/A

Platform Description

11.21 aaa log enable

Use this command to enable the system to print the syslog informing AAA authentication success. Use the **no** form of this command to restore the default setting.

aaa log enable

no aaa log enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable the system to print the syslog informing aaa authentication success.

Configuration Examples The following example disables the system to print the syslog informing aaa authentication success.

```
FS(config)# no aaa log enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

11.22 aaa log rate-limit

Use this command to set the rate of printing the syslog informing AAA authentication success.

Use the **no** form of this command to restore the default printing rate.

aaa log rate-limit *num*

no aaa log rate-limit

Parameter Description

Parameter	Description
num	The number of syslog entries printed per second. The range is from 0 to 65,535. 0 indicates the printing rate is not limited.

Defaults

The default is 5.

Command Mode

Global configuration mode

Usage Guide

Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate.

Configuration Examples

The following example sets the rate of printing the syslog informing AAA authentication success to 10.

```
FS(config)# aaa log rate-limit 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

11.23 aaa new-model

Use this command to enable the FSOS AAA security service.

Use the **no** form of this command to restore the default setting.

aaa new-model

no aaa new-model

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.

Configuration Examples

The following example enables the AAA security service.

```
FS(config)# aaa new-model
```

Related Commands

Command	Description
aaa authentication	Defines a user authentication method list.
aaa authorization	Defines a user authorization method list.
aaa accounting	Defines a user accounting method list.

Platform Description

N/A

11.24 access-limit

Use this command to configure the number of users limit for the domain, which is only valid for the IEEE802.1 users.

Use the **no** form of this command to restore the default setting.

access-limit *num*

no access-limit

Parameter Description

Parameter	Description
num	The number used for the user limitation is only valid for the IEEE802.1 users.

Defaults

By default, no number of users is limited.

Command Mode

Domain configuration mode

Usage Guide

This command limits the number of users for the domain.

Configuration Examples

The following example sets the number of users to 20 for the domain named FS.com.

```
FS(config)# aaa domain FS.com
FS(config-aaa-domain)# access-limit 2
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Switchover the user level.
show aaa domain	Defines a local user database.

Platform Description

N/A

11.25 accounting network

Use this command to configure the Network accounting list.

Use the **no** form of this command to restore the default setting.

accounting network { **default** | *list-name* }

no accounting network

Parameter Description

Parameter	Description
default	Uses this parameter to specify the default method list.
list-name	The name of the network accounting list

Defaults

With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.

Command Mode

Domain configuration mode

Usage Guide

Use this command to configure the Network accounting method list for the specified domain.

Configuration Examples

The following example sets the Network accounting method list for the specified domain.

```
FS(config)# aaa domain FS.com
FS(config-aaa-domain)# accounting network default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description

N/A

11.26 authentication dot1x

Use this command to configure the IEEE802.1x authentication list.

Use the **no** form of this command to restore the default setting.

authentication dot1x { **default** | *list-name* }

no authentication dot1x

Parameter Description

Parameter	Description
default	Uses this parameter to specify the default method list
list-name	The name of the specified method list

Defaults With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command Mode Domain configuration mode

Usage Guide Specify an IEEE802.1x authentication method list for the domain.

Configuration Examples The following example sets an IEEE802.1x authentication method list for the specified domain.

```
FS(config)# aaa domain FS.com
FS(config-aaa-domain)# authentication dot1x default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description N/A

11.27 authorization network

Use this command to configure the Network authorization list.

Use the **no** form of this command to restore the default setting.

authorization network { **default** | *list-name* }

no authorization network

Parameter Description

Parameter	Description
default	Uses this parameter to specify the default method list.
list-name	The name of the specified method list

Defaults With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command Mode Domain configuration mode

Usage Guide Specify an authorization method list for the domain.

Configuration Examples The following example sets an authorization method list for the specified domain.

```
FS(config)# aaa domain FS.com
FS(config-aaa-domain)# authorization network default
```

Related

Command	Description

Commands

aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description N/A

11.28 clear aaa local user lockout

Use this command to clear the lockout user list.

clear aaa local user lockout { **all** | **user-name** *word* }

Parameter Description

Parameter	Description
all	Indicates all locked users.
user-name *word*	Indicates the ID of the locked User.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear all the user lists or a specified user list.

Configuration Examples The following example clears the lockout user list.

```
FS(config)# clear aaa local user lockout all
```

Related Commands

Command	Description
show running-config	Displays the current configuration of the switch.
show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description N/A

11.29 show aaa accounting update

Use this command to display the accounting update information.

show aaa accounting update

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the accounting update interval and whether the accounting update is enabled.

Configuration Examples

The following example displays the accounting update information.

```
FS# show aaa accounting update
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.

Platform Description

N/A

11.30 show aaa domain

Use this command to display all current domain information.

show aaa domain [**default** | *domain-name*]

Parameter Description

Parameter	Description
default	Displays the default domain.
domain-name	Displays the specified domain.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

If no domain-name is specified, all domain information will be displayed.

Configuration Examples

The following example displays the domain named domain.com.

```
FS(config)# show aaa domain domain.com
=============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
  authentication dot1x default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.

aaa domain enable	Enables the domain-name-based AAA service.

Platform Description N/A

11.31 group

Use this command to display all the server groups configured for AAA.

show aaa group

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following command displays all the server groups.

```
FS# show aaa group
Type         Reference   Name
---------- ---------- ----------
radius        1            radius
tacacs+       1            tacacs+
radius        1            dot1x_group
radius        1            login_group
radius        1            enable_group
```

Related Commands

Command	Description
aaa group server	Configures the AAA server group.

Platform Description N/A

11.32 show aaa lockout

Use this command to display the lockout configuration.

show aaa lockout

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the lockout configuration.

Configuration Examples

The following example displays the lockout configuration.

```
FS# show aaa lockout
Lock tries:        3
Lock timeout:    15 minutes
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

11.33 show aaa method-list

Use this command to display all AAA method lists.

show aaa method-list

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display all AAA method lists.

Configuration Examples

The following example displays the AAA method list.

```
FS# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local    group angel group rain none
aaa authentication enable default group radius
Accounting method-list
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorization network default group radius
```

Related Commands

Command	Description
aaa authentication	Defines a user authentication method list
aaa authorization	Defines a user authorization method list
aaa accounting	Defines a user accounting method list

Platform Description

N/A

11.34 show aaa user

Use this command to display AAA user information.

show aaa user { all | lockout | by-id *session-id* **| by-name** *user-name* **}**

Parameter Description

Parameter	Description
all	Displays all AAA user information.
lockout	Displays the locked AAA user information.
by-id *session-id*	Displays the information of the AAA user that with a specified session ID.
by-name *user-name*	Displays the information of the AAA user with a specified user name.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display AAA user information.

Configuration Examples

The following example displays AAA user information.

```
FS#show aaa user all
-----------------------------
            Id ----- Name
  2345687901          wwxy
-----------------------------
FS# show aaa user by-id 2345687901
-----------------------------
            Id ----- Name
  2345687901          wwxy
FS# show aaa user by-name wwxy
-----------------------------
```

```
         Id ----- Name
 2345687901         wwxy
-----------------------------


FS# show aaa user lockout


Name                                     Tries       Lock        Timeout(min)
-------------------------------- ---------- ---------- ------------
FS#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

11.35 state

Use this command to set whether the configured domain is valid.

Use the **no** form of this command to restore the default setting.

state { **block** | **active** }

no state

Parameter Description

Parameter	Description
block	The configured domain is invalid.
active	The configured domain is valid.

Defaults

The default is active.

Command Mode

Domain configuration mode

Usage Guide

Use this command to set whether the specified configured domain is valid.

Configuration Examples

The following example sets the configured domain to be invalid.

```
FS(config)# aaa domain FS.com
FS(config-aaa-domain)# state block
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain enable	Displays the domain configuration.

Platform Description

N/A

11.36 username-format

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Use the **no** form of this command to restore the default setting.

username-format { **without-domain** | **with-domain** }

no username-format

Parameter Description

Parameter	Description
without-domain	Sets the user name without the domain information.
with-domain	Sets the user name with the domain information.

Defaults

The default is without-domain.

Command Mode

Domain configuration mode

Usage Guide

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Configuration Examples

The following example sets the user name without the domain information.

```
FS(config)# aaa domain FS.com
FS(config-aaa-domain)# username-domain without-domain
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description

N/A

12 RADIUS Commands

12.1 aaa group server radius

Use this command to enter AAA server group configuration mode.

Use the **no** form of this command to restore the default setting.

aaa group server radius *name*

no aaa group server radius *name*

Parameter Description

Parameter	Description
name	Server group name. Keywords “radius” and “tacacs +” are excluded as they are the default RADIUS and TACACS+ server group names.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to configure a RADIUS AAA server group.

Configuration Examples The following example configures a RADIUS AAA server group named ss.

```
FS(config)# aaa group server radius ss
FS(config-gs-radius)# end
FS# show aaa group
Type       Reference   Name
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          ss
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.2 ip oob

Use this command to specify the MGMT port used in the TACACS+ server group.

Use the **no** form of this command to restore the default setting.

ip oob

no ip oob

Parameter Description

Parameter	Description

Defaults N/A

Command Mode server group configuration mode

Usage Guide Use the **aaa group server radius** command to enter **radius** server group configuration mode. If no port is specified as the MGMT port. MGMT Port 0 is default.

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description MGMT ports are supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME but not on EG2000K, EG2000L, or EG2000F.

12.3 ip radius source-interface

Use this command to specify the source IP address for the RADIUS packet.

Use the **no** form of this command to delete the source IP address for the RADIUS packet.

ip radius source-interface *interface-name*

no radius source-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Interface that the source IP address of the RADIUS packet belongs to.

Defaults The source IP address of the RADIUS packet is set by the network layer.

Command mode Global configuration mode

Usage Guide In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

Configuration The following example specifies that the RADIUS packet obtains an IP address from the fastEthernet 0/0 interface

Examples and uses it as the source IP address of the RADIUS packet.

```
FS(config)# ip radius source-interface fastEthernet 0/0
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS server.
ip address	Configures the IP address of the interface.

Platform Description N/A

12.4 radius set qos cos

Use this command to set the QoS value sent by the RADIUS server as the CoS value of the interface. Use the **no** form of this command to restore the default setting.

radius set qos cos

no radius set qos cos

Parameter Description

Parameter	Description
N/A	N/A

Defaults Set the QoS value sent by the RADIUS server as the DSCP value.

Command Mode Global configuration mode.

Usage Guide

Configuration Examples The following example sets the QoS value sent by the RADIUS server as the CoS value of the interface:

```
FS(config)# radius set qos cos
```

Related Commands

Command	Description
radius vendor-specific extend	Extends RADIUS as not to differentiate the IDs of private vendors.

Platform Description N/A

12.5 radius support cui

Use this command to enable RADIUS to support the cui function.

Use the **no** form of this command to restore the default setting.

radius support cui

no radius support cui

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to enable RADIUS to support the cui function.

Configuration Examples

The following example enables RADIUS to support the cui function.

```
FS(config)# radius support cui
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.6 radius vendor-specific attribute support

Use this command to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor.

Use the **no** form of this command to configure that RADIUS accounting request packets do not carry the private attribute of a specified vendor.

radius vendor-specific attribute support { cisco | huawei | ms}

no radius vendor-specific attribute support { cisco | huawei | ms}

Parameter Description

Parameter	Description
cisco	Indicates the private attribute of Cisco.
huawei	Indicates the private attribute of Huawei.
ms	Indicates the private attribute of Microsoft.

Defaults

By default, RADIUS accounting request packets carry the private attribute of a specified vendor.

Command Mode

Global configuration mode

Usage Guide

This command is used to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.

Configuration Examples

1. The following example configures that RADIUS accounting request packets carry the private attribute of Huawei.

```
FS(config)# radius vendor-specific attribute support huawei
```

2. The following example configures that RADIUS accounting request packets do not carry the private attribute of Huawei.

```
FS(config)# no radius vendor-specific attribute support huawei
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.7 radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors.

Use the **no** form of this command to restore the default setting.

radius vendor-specific extend

no radius vendor-specific extend

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Only the private vendor IDs of FS are recognized.

Command Mode

Global configuration mode

Usage Guide

This command is used to identify the attributes of all vendor IDs by type.

Configuration Examples

The following example extends RADIUS so as not to differentiate the IDs of private vendors:

```
FS(config)# radius vendor-specific extend
```

Related Commands

Command	Description
radius attribute	Configures vendor type.

radius set qos cos	Sets the QoS value sent by the RADIUS server as the cos value of the interface.

Platform Description N/A

12.8 radius-server account attribute

Use this command to enable account-request packets to contain a specified RADIUS attribute.

Use the **no** or **default** form of this command to restore the default setting.

radius-server account attribute *type* **package**

no radius-server account attribute *type* **package**

default radius-server account attribute *type* **package**

Use this command to disable account-request packets to contain a specified RADIUS attribute.

Use the **no** or **default** form of this command to restore the default setting.

radius-server account attribute *type* **unpackage**

no radius-server account attribute *type* **unpackage**

default radius-server account attribute *type* **unpackage**

Parameter Description

Parameter	Description
type	RADIUS attribute in the range from 1 to 255

Defaults RFC-compliant

Command Mode Global configuration mode

Usage Guide Use this command to enable or disable account-request packets to contain a specified RADIUS attribute.

Configuration Examples The following example disables account-request packets to contain attribute NAS-PORT-ID.

```
FS(config)# radius-server account attribute 87 unpackage
```

Platform Description N/A

12.9 radius-server account update retransmit

Use this command to configure accounting update packet retransmission for the Web authentication user.

Use the **no** form of this command to restore the default setting,

radius-server account update retransmit

no radius-server account update retransmit

Parameter

Parameter	Description

Description

N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to configure accounting update packet retransmission for the Web authentication user exclusively.

Configuration Examples The following example configures accounting update packet retransmission for the Web authentication user.

```
FS(config)#radius-server account update retransmit
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

12.10 radius-server authentication vendor

Use this command to enable access-request packets to contain vendor-specific RADIUS attributes.

Use the **no** or **default** form of this command to restore the default setting.

radius-server authentication vendor *vendor_name* **package**

no radius-server authentication vendor *vendor_name* **package**

default radius-server authentication vendor *vendor_name* **package**

Parameter Description

Parameter	**Description**
vendor_name	**cmcc/ microsoft/cisco**

Defaults Access-request packets do not contain vendor- specific RADIUS attributes by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable access-request packets to contain vendor- specific RADIUS attributes.

Configuration Examples The following example enables access-request packets to contain “cmcc”.

```
FS(config)# radius-server authentication vendor cmcc package
```

Platform N/A

Description

12.11 radius-server attribute class

Use this command to analyze the flow control value of the RADIUS CLASS attributes.

Use the **no** form of this command to restore the default setting.

radius-server attribute class user-flow-control { **format-16bytes** | **format-32bytes** }

no radius-server attribute class user-flow-control

Parameter Description

Parameter	Description
user-flow-control	Analyzes flow control value in the CLASS attribute.
format-16bytes	Sets the format of flow control value to 16 bytes.
format-32bytes	Sets the format of flow control value to 32 bytes.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is required if the server pushes the flow control value through the CLASS attribute.

Configuration Examples

The following example analyzes the flow control value of the CLASS attribute and sets the format to 32 bytes.

```
FS(config)#radius-server attribute class user-flow-control format-32bytes
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.12 radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute.

Use the **no** form of this command to restore the default setting.

radius-server attribute 31 mac format { **ietf** | **normal** | **unformatted** }

no radius-server attribute 31 mac format

Parameter Description

Parameter	Description
ietf	The standard format specified by the IETF RFC3580. ‘-‘is used as the separator, for example: 00-D0-F8-33-22-AC.
normal	Normal format representing the MAC address. ;.’is used as the separator. For example: 00d0.f833.22ac.
unformatted	No format and separator. By default, unformatted is

	used. For example: 00d0f83322ac.

Defaults The default format is unformatted.

Command Mode Global configuration mode

Usage Guide Some RADIUS security servers (mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

Configuration Examples The following example defines the RADIUS Calling-Station-ID attribute as IETF format.

```
FS(config)# radius-server attribute 31 mac format ietf
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS server.

Platform Description N/A

12.13 radius-server authentication attribute

Use this command to enable access-request packets to contain a specified RADIUS attribute.

Use the **no** or **default** form of this command to restore the default setting.

radius-server authentication attribute *type* **package**

no radius-server authentication attribute *type* **package**

default radius-server authentication attribute *type* **package**

Use this command to disable access-request packets to contain a specified RADIUS attribute.

Use the **no** or **default** form of this command to restore the default setting.

radius-server authentication attribute *type* **unpackage**

no radius-server authentication attribute *type* **unpackage**

default radius-server authentication attribute *type* **unpackage**

Parameter Description

Parameter	Description
type	RADIUS attribute in the range from 1 to 255

Defaults RFC-compliant

Command Mode Global configuration mode

Usage Guide Use this command to enable access-request packets to contain a specified RADIUS attribute.

Configuration Examples The following example disables access-request packets to contain attribute NAS-PORT-ID.

```
FS(config)# radius-server authentication attribute 87 unpackage
```

Platform Description N/A

12.14 radius-server authentication vendor

Use this command to enable access-request packets to contain vendor-specific RADIUS attributes.

- Use the **no** or **default** form of this command to restore the default setting.

radius-server authentication vendor [cmcc | microsoft | cisco] package

no radius-server authentication vendor *vendor_name* **package**

default radius-server authentication vendor *vendor_name* **package**

Parameter Description

Parameter	Description
cmcc | microsoft | cisco	**Vendor name, cmcc/ microsoft/cisco**

Defaults Access-request packets do not contain vendor- specific RADIUS attributes by default.

Command Mode Global configuration mode

Usage Guide Use this command to enable access-request packets to contain vendor- specific RADIUS attributes.

Configuration Examples The following example enables access-request packets to contain “cmcc”.

```
FS(config)# radius-server authentication vendor cmcc package
```

Platform Description N/A

12.15 radius-server dead-criteria

Use this command to configure criteria on a device to determine that the Radius server is unreachable.

Use the **no** form of this command to restore the default setting.

radius-server dead-criteria { **time** *seconds* [**tries** *number*] **|** **tries** *number* }

no radius-server dead-criteria { **time** *seconds* [**tries** *number*] **|** **tries** *number* }

Parameter Description

Parameter	Description
time *seconds*	Configures the timeout value. If the device does not receive a correct response packet from the Radius server within the specified time, the Radius server is considered to be unreachable. The value is in the range from 1 to 120 in the unit of seconds.
tries *number*	Configures the successive timeout times. When sending a request from the device to the Radius server times out for the specified times, the device considers that the Radius server is unreachable. The value is in the range from

	1 to 100 in the unit of seconds.

Defaults The default **time** *seconds* is 60 and **tries** *number* is 10.

Command Mode Global configuration mode

Usage Guide If a Radius server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

Configuration Examples The following example sets the timeout to 120 seconds and timeout times to 20.

```
FS(config)# radius-server dead-criteria time 120 tries 20
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server deadtime	Defines the duration when a device stops sending any requests to an unreachable Radius server.
radius-server timeout	Defines the timeout for the packet re-transmission.

Platform Description N/A

12.16 radius-server deadtime

Use this command to configure the duration when a device stops sending any requests to an unreachable Radius server.

Use the **no** form of this command to restore the default setting.

radius-server deadtime *minutes*

no radius-server deadtime

Parameter Description

Parameter	Description
minutes	Defines the duration in minutes when the device stops sending any requests to the unreachable Radius server. The value is in the range from 1 to 1,440 in the unit of minutes.

Defaults The default value of minutes is 0, that is, the device keeps sending requests to the unreachable Radius server.

Command Mode Global configuration mode

Usage Guide If active Radius server detection is enabled on the device, the time parameter of this command does not take effect on the Radius server. Otherwise, the Radius server becomes reachable when the duration set by this command is shorter than the unreachable time.

Configuration Examples

The following example sets the duration when the device stops sending requests to 1 minute.

```
FS(config)# radius-server deadtime 1
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server dead-criteria	Defines the criteria to determine that a Radius server is unreachable.

Platform Description

N/A

12.17 radius-server host

Use this command to specify a RADIUS security server host.

Use the **no** form of this command to restore the default setting.

radius-server host [**oob**] { *ipv4-address* | *ipv6-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*]

no radius-server host { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
oob	Specifies an MGMT port as the source port for TACACS+ communication. The default is MGMT Port 0.
Ipv4-address	IPv4 address of the RADIUS security server host.
Ipv6-address	IPv4 address of the RADIUS security server host.
auth-port	UDP port used for RADIUS authentication.
port-number	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
acct-port	UDP port used for RADIUS accounting.
port-number	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
test username *name*	(Optional) Enables the active detection to the RADIUS security server and specify the username used by the active detection.
idle-time *time*	(Optional) Sets the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
ignore-auth-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
ignore-acct-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.

key [**0** | **7**] *text-string*	Configure a shared key for the server. The type of encryption can be specified. 0 is no encryption and 7 is simple encryption. The default is 0.

Defaults No RADIUS host is specified by default.

Command Mode Global configuration mode

Usage Guide In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

Configuration Examples The following example defines a RADIUS security server host:

```
FS(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
FS(config)# radius-server host 192.168.100.1 test username viven idle-time 60 ignore-acct-port
```

The following example defines a RADIUS security server host in the IPv6 environment

```
FS(config)# radius-server host 3000::100
```

Related Commands

Command	Description
aaa authentication	Defines the AAA authentication method list
radius-server key	Defines a shared password for the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.

Platform Description MGMT ports are supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME but not on EG2000K, EG2000L, or EG2000F.

12.18 radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server.

Use the **no** form of this command to restore the default setting.

radius-server key [**0 | 7**] *text-string*

no radius-server key

Parameter Description

Parameter	Description
text-string	Text of the shared password
0 | 7	Password encryption type.

	0: no encryption; 7: Simply-encrypted.

Defaults No shared password is specified by default.

Command Mode Global configuration mode.

Usage Guide A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

Configuration Examples The following example defines the shared password **aaa** for the RADIUS security server:

```
FS(config)# radius-server key aaa
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server timeout	Defines the timeout for the RADIUS packet.

Platform Description N/A

12.19 radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond.

Use the **no** form of this command to restore the default setting.

radius-server retransmit *retries*

no radius-server retransmit

Parameter Description

Parameter	Description
retries	Number of retransmissions in the range from 1 to 100.

Defaults The default is 3.

Command Mode Global configuration mode.

Usage Guide AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

Configuration Examples

The following example sets the number of retransmissions to 4.

```
FS(config)# radius-server retransmit 4
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the timeout for the RADIUS packet.

Platform Description

N/A

12.20 radius-server source-port

Use this command to configure the source port to send RADIUS packets.

Use the **no** form of this command to restore the default setting.

radius-server source-port *port*

no radius-server source-port

Parameter Description

Parameter	Description
port	The port ID, in the range from 0 to 65535.

Defaults

The default is a random number.

Command Mode

Global configuration mode

Usage Guide

The source port is random by default. This command is used to specify a source port.

Configuration Examples

The following example configures source port 10000 to send RADIUS packets.

```
FS(config)# radius-server source-port 10000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.21 radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet.

Use the **no** form of this command to restore the default setting.

radius-server timeout *seconds*

no radius-server timeout

Parameter Description

Parameter	Description
seconds	Timeout in the range from 1 to 1,000 in the unit of seconds.

Defaults The default is 5 seconds.

Command Mode Global configuration mode

Usage Guide This command is used to change the timeout of packet retransmission.

Configuration Examples The following example sets the timeout to 10 seconds.

```
FS(config)# radius-server timeout    10
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of the RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.

Platform Description N/A

12.22 server auth-port acct-port

Use this command to add the server of the AAA server group.

Use the **no** form of this command to restore the default setting.

server { *ipv4-addr* } [**auth-port** *port1*] [**acct-port** *port2*]

no server { *ipv4-addr* } [**auth-port** *port1*] [**acct-port** *port2*]

Parameter Description

Parameter	Description
ip-addr	Server IP address
port1	Server authentication port
port2	Server accounting port

Defaults No server is configured by default.

Command Mode

Server group configuration mode

Usage Guide

N/A

Configuration Examples

The following example adds server 192.168.4.12 to server group ss and sets the accounting port and authentication port to 5 and 6 respectively.

```
FS(config)# aaa group server radius ss
FS(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
FS(config-gs-radius)# end
FS# show aaa group
Type          Reference   Name
---------- ---------- ----------
radius        1             radius
tacacs+       1             tacacs+
radius        1             ss
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.23 show radius acct statistics

Use this command to display RADIUS accounting statistics.

show radius acct statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays RADIUS accounting statistics.

```
FS#show radius acct statistics
Accounting Servers:

Server Index.................................... 1
Server Address.................................. 192.168.1.1
Server Port...................................... 1813
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 1
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests........
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.24 show radius attribute

Use this command to display standard Radius attributes.

show radius attribute

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples

The following example displays standard RADIUS attributes.

```
FS#sh radius attribute
type                 implicate
----                 ---------
1..........User-Name
2..........User-Password
3..........Chap-Password
4..........NAS-Ip-Addr
5..........Nas-Ip-Port
6..........Service-Type
7..........Framed-Protocol
8..........Frame-Ip-Address
9..........Framed-Ip-Mask
10..........Framed-Routing
11..........Filter-Id
12..........Framed-Mtu
13..........Framed-Compress
```

```
14..........Login-Ip-Host
15..........Login-Service
16..........Login-Tcp-Port
18..........Reply-Message
19..........Callback-Num
20..........Callback-Id
22..........Framed-Route
23..........Framed-IPX-Network
24..........State
25..........Class
26..........Vendor-Specific
27..........Session-Timeout
28..........Idle-Timeout
29..........Termination-Action
30..........Called-Station-Id
31..........Calling-Station-Id
32..........Nas-Id
33..........Proxy-State
34..........Login-LAT-Service
35..........Login-LAT-Node
36..........Login-LAT-Group
37..........Framed-AppleTalk-Link
38..........Framed-AppleTalk-Net
39..........Framed-AppleTalk-Zone
40..........Acct-Status-Type
41..........Acct-Delay-Time
42..........Acct-Input-Octets
43..........Acct-Output-Octets
44..........Acct-Session-Id
45..........Acct-Authentic
46..........Acct-Session-Time
47..........Acct-Input-Packet
48..........Acct-Output-Packet
49..........Acct-Terminate-Cause
50..........Acct-Multi-Session-ID
51..........Acct-Link-Count
52..........Acct-Input-Gigawords
53..........Acct-Output-Gigawords
60..........Chap-Challenge
61..........Nas-Port-Type
62..........Port-Limit
63..........Login-Lat-Port
64..........Tunnel-Type
65..........Tunnel-Medium-Type
```

```
66..........Tunnel-Client-EndPoint
67..........Tunnel-Service-EndPoint
79..........eap msg
80..........Message-Authenticator
81..........group id
85..........Acct-Interim-Interval
87..........Nas-Port-Id
89..........cui
95..........Nas-Ipv6-Addr
96..........Framed-Interface-Id
```

Platform Description N/A

12.25 show radius auth statistics

Use this command to display RADIUS authentication statistics.

show radius auth statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays RADIUS authentication statistics.

```
FS#show radius auth statistics
Authentication Servers:

Server Index.................................... 1
Server Address.................................. 192.168.1.1
Server Port..................................... 1812
Msg Round Trip Time............................. 0 (msec)
First Requests.................................. 0
Retry Requests.................................. 0
Accept Responses................................ 0
Reject Responses................................ 0
Challenge Responses............................. 0
Malformed Msgs.................................. 0
```

```
Bad Authenticator Msgs........................... 0
Pending Requests................................ 0
Timeout Requests................................ 0
Unknowntype Msgs................................ 0
Other Drops..................................... 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.26 show radius group

Use this command to display RADIUS server group configuration.

show radius group

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays RADIUS server group configuration.

```
FS#show radius group
==========Radius group radius==========
Vrf:not-set
Server:192.168.1.1
Server key:FS
Authentication port:1812
Accounting port:1813
State:Active
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

12.27 show radius parameter

Use this command to display global RADIUS server parameters.

show radius parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays global RADIUS server parameters.

```
FS# show radius parameter
Server Timout:      5 Seconds
Server Deadtime: 0 Minutes
Server Retries:    3
Server Dead Critera:
Time:              10 Seconds
Tries:             10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.28 show radius server

Use this command to display the configuration of the RADIUS server.

show radius server

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the configuration of the RADIUS server.

```
FS# show radius server
Server IP:        192.168.4.12
Accounting    Port:    23
Authen    Port:         77
Test Username:        viven
Test Idle Time:      10 Minutes
Test Ports:                Authen
Server State:          Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0

Server IP:        192.168.4.13
Accounting Port:    45
Authen    Port:         74
Test Username:        <Not Configured>
Test Idle Time:      60 Minutes
Test Ports:                Authen and Accounting
Server State:          Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the packet transmission timeout.

Platform

N/A

Description

12.29 show radius vendor-specific

Use this command to display the configuration of the private vendors.

show radius vendor-specific

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the configuration of the private vendors.

```
FS#show radius vendor-specific
id      vendor-specific          type-value
----- -------------------- ----------
1        max-down-rate              1
2        port-priority              2
3        user-ip                    3
4        vlan-id                    4
5        last-supplicant-vers 5
ion
6        net-ip                     6
7        user-name                  7
8        password                   8
9        file-directory             9
10       file-count                 10
11       file-name-0                11
12       file-name-1                12
13       file-name-2                13
14       file-name-3                14
15       file-name-4                15
16       max-up-rate                16
17       current-supplicant-version 17
18       flux-max-high32            18
19       flux-max-low32             19
20       proxy-avoid                20
21       dialup-avoid               21
```

```
22        ip-privilege            22
23        login-privilege         42
27        ipv4-multicast-addre 87
ss
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the packet transmission timeout.

Platform Description

N/A

13 TACACS+ Commands

13.1 aaa group server tacacs+

Use this command to configure different groups of TACACS+ server hosts.

Use the **no** form of this command to remove a specified TACACS server group.

aaa group server tacacs+ *group_name*

no aaa group server tacacs+ *group_name*

Parameter Description

Parameter	Description
group_name	TACACS+ server group name, which cannot be **radius** or **tacacs+** The two names are the built-in group name.

Defaults

No TACACS+ server group is configured.

Command Mode

Global configuration mode

Usage Guide

After you group different TACACS+ servers, the tasks of authentication, authorization and accounting can be implemented by different server groups.

Configuration Examples

The following example configures a TACACS+ server group named tac1, and configures a TACACS+ server with IP address 1.1.1.1 in this group:

```
FS(config)#aaa group server tacacs+ tac1
FS(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands

Command	Description
server	Configures server list of TACACS+ server group.
ip vrf forwarding	Configures VRF name supported by TACACS+ server group.

Platform Description

N/A

13.2 ip oob

Use this command to specify the MGMT port used in the TACACS+ server group.

Use the **no** form of this command to restore the default setting.

ip oob

no ip oob

Parameter Description

Parameter	Description

Defaults N/A

Command Mode TACACS+ server group configuration mode

Usage Guide Use the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode. No MGMT port is specified by default.

Configuration Examples The following example specifies MGMT port 1 used in the TACACS+ server group.

```
FS(config)# aaa group server tacacs+ ss
FS(config-gs-tacacs+)# server 1.1.1.1
FS(config-gs-tacacs+)# ip oob via mgmt 1
```

Platform Description N/A

13.3 ip tacacs source-interface

Use this command to use the IP address of a specified interface for all outgoing TACACS+ packets. Use the **no** form of this command to disable use of the specified interface IP address.

ip tacacs source-interface *interface-name*

no ip tacacs source-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Interface for the outgoing TACACS+ packets

Defaults The source IP address of TACACS+ packets is set on the network layer.

Command Mode Global configuration mode

Usage Guide To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.

This command specifies the primary IP address of the specified interface as the source address of TACACS+ packets on Layer 3 devices.

Configuration Examples The following example specifies the IP address of GigabitEthernet 0/0 for the outgoing TACACS+ packets.

```
FS(config)# ip tacacs source-interface gigabitEthernet 0/0
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ server.
ip address	Configures the IP address of an interface.

Platform Description

N/A

13.4 server

Use this command to configure the IP address of the TACACS+ server for the group server.

Use the **no** form of this command to remove the TACACS+ server.

server { *ipv4-address* }

no server { *ipv4-address* }

Parameter Description

Parameter	Description
ipv4-address	IPv4 address of the TACACS+ server

Defaults

No TACACS+ server is configured by default.

Command Mode

TACACS+ server group configuration mode

Usage Guide

You must configure the **aaa group server tacacs+** command before configuring this command.

To configure server address in TACACS+ group server, you must use the **tacacs-server host** command in global configuration mode.

If there is no response from the first host entry, the next host entry is tried.

Configuration Examples

The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group.

```
FS(config)#aaa group server tacacs+ tac1
FS(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands

Command	Description
aaa group server tacacs+	Configures a TACACS+ server group.

Platform Description

N/A

13.5 show tacacs

Use this command to display the TACACS+ server configuration.

show tacacs

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the TACACS+ server configuration.

```
FS# show tacacs
Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.

Platform Description

N/A

13.6 tacacs-server host

Use this command to configure a TACACS+ host.

Use the **no** form of this command to remove the TACACS+ host.

tacacs-server host [**oob**] { *ipv4-address* | *ipv6-address* } [**port** *integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]

no tacacs-server host {*ipv4-address* }

Parameter Description

Parameter	Description
ip-address	IPv4 address of the TACACS+ host
ipv6-address	IPv6 address of the TACACS+ host
oob	Specifies an MGMT port as the source port for TACACS+ communication.
port *integer*	Port number of the server. The range is from 1 to 65,535. The default is 49.
timeout *integer*	Timeout time of TACACS+ host. The range is from 1 to 1,000.

key *string*	Configures an authentication and encryption key. The value can be 0 or 7. 0 indicates no encryption, while 7 indicates simple encryption. The default is 0.

Defaults No TACACS+ host is specified by default.

Command Mode Global configuration mode

Usage Guide The TACACS+ host must be configured to implement AAA security service You can use this command to configure one or multiple TACACS+ hosts.

Configuration Examples The following example configures a TACACS+ host.

```
FS(config)# tacacs-server host 192.168.12.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description MGMT ports are supported on EG2000CE, EG2000SE, EG2000P, EG2000GE, EG2000XE, EG2000UE, EG3000XE, EG3000UE, EG3000GE and EG3000ME but not on EG2000K, EG2000L, or EG2000F.

13.7 tacacs-server key

Use this command to configure the authentication encryption key used for TACACS+ communications between the access server and the TACACS+ server.

Use the **no** form of this command to remove the authentication encryption key.

tacacs-server key [**0** | **7**] *string*

no tacacs-server key

Parameter Description

Parameter	Description
string	Key string
0 | 7	Encryption type of key 0 indicates no encryption; 7 indicate simple encryption.

Defaults No authentication encryption key is configured by default.

Command Mode Global configuration mode

Usage Guide Use command to configure a global authentication and encryption key for TACACS+ communication. Use the **key** parameter in the **tacacs-server host** command to configure a server-based key.

Configuration Examples

The following example defines the authentication encryption key of TACACS+ server as aaa:

```
FS(config)# tacacs-server key aaa
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ host.

Platform Description

N/A

13.8 tacacs-server timeout

Use this command to set the interval for which the server waits for a server host to reply. Use the **no** form of this command to restore the default timeout interval.

tacacs-server timeout *seconds*

no tacacs-server timeout

Parameter Description

Parameter	Description
seconds	Timeout interval in the range from 1 to 1,000 in the unit of seconds

Defaults

The default is 5 seconds.

Command Mode

Global configuration mode

Usage Guide

Use command to configure a global timeout interval. Use the **timeout** parameter in the **tacacs-server host** command to configure a server-based interval.

Configuration Examples

The following example configures the timeout interval to 10 seconds.

```
FS(config)# tacacs-server timeout 10
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.

Platform Description

N/A

14 Web Authentication Commands

14.1 accounting

Use this command to set an accounting method for the template.

Use the **no** form of this command to restore the default setting.

accounting { *method-list* }

no accounting

Parameter Description

Parameter	Description
method-list	Name of the method list

Defaults N/A

Command Mode Template configuration mode

Usage Guide The *method-list* parameter in this command should be consistent with network accounting list name configured in AAA.

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.2 authentication

Use this command to set an authentication method for the template.

Use the **no** form of this command to restore the default setting.

authentication { *method-list* }

no authentication

Parameter Description

Parameter	Description
method-list	Name of the method list

Defaults N/A

Command Mode

Template configuration mode

Usage Guide

The *method-list* parameter in this command should be consistent with the Web authentication method list configured in AAA.

The first generation authentication does not support the authentication method list configuration.

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.3 bindmode

Use this command to set a binding mode for the template.

Use the **no** form of this command to restore the default setting.

bindmode

no bindmode

Parameter Description

Parameter	Description

Defaults

The default is **ip-mac-mode**.

Command Mode

Template configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.4 clear web-auth direct-arp

Use this command to clear all ARP resources exempt from authentication.

clear web-auth direct-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example clears all ARP resources exempt from authentication.

```
FS# clear web-auth direct-arp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.5 clear web-auth direct host

Use this command to clear all authentication-exempted users.

clear web-auth direct-host [range]

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example clears all authentication-exempted users.

```
FS# clear web-auth direct-host
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.6 clear web-auth direct-site

Use this command to clear all authentication-exempted network resources.

clear web-auth direct-site

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears all authentication-exempted network resources.

```
FS# clear web-auth direct-site
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.7 clear web-auth group

Use this command to clear all group information.

clear web-auth group

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example clears all group information.

```
FS# clear web-auth group
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

14.8 clear web-auth user

Use this command to force the user to go offline.

clear web-auth user { **all** | **ip {** *ip-address* } | **mac** *mac-address* **| name** *name-string* | **session-id** *num* }

Parameter Description

Parameter	**Description**
ip-address	Specifies the user’s IPv4 address.
mac-address	Specifies the user’s MAC address.
name-string	Specifies the user name.
num	Specifies the user’s AAA session ID.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example forces all users to go offline.

```
FS(config) clear web-auth user all
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

14.9 fmt

Use this command to set the URL redirection format in the second template configuration mode.

fmt { cmcc-ext1 | cmcc-ext2 | cmcc-mtx | cmcc-normal | cmcc-ext3 | FS | custom}

Use this command to set the URL redirection format in the first template configuration mode.

fmt { ace | FS | custom }

Use this command to set the custom URL redirection format in the first & second template configuration modes.

fmt custom [encry { md5 | des | des_ecb | des_ecb3 | none }] [user-ip *userip-str* **] [user-mac** *usermac-str* **mac-format [dot | line | none]] [user-vid** *uservid-str* **]** [**user-id** *userid-str*] **[nas-ip** *nasip-str* **] [nas-id** *nasid-str* **] [nas-id2** *nasid2-str* **] [ac-name** *acname-str* **] [ac-name** acname-str **] [ap-mac** *apmac-str* **mac-format [dot | line | none]] [url** *url-str* **] [ssid** *ssid-str* **] [port** *port-str* **] [ac-serialno** *ac-sno-str* **] [ap-serialno** *ap-sno-str* **]**

Use the **no** form of **fmt custom** command to remove the custom URL redirection format.

no fmt custom [user-ip] [user-mac] [user-vid] [**user-id] [nas-ip] [nas-id] [nas-id2] [ac-name] [ap-mac] [url] [ssid] [port] [ac-serialno] [ap-serialno] [additional]**

Parameter Description

Parameter	**Description**
cmcc-ext1	Extended CMCC format
cmcc-ext2	Liaoning CMCC format
cmcc-mtx	CMCC format for AC manufacturers
cmcc-normal	Standard CMCC format
ace	Supports ACE correlation.
FS	FS format
custom	Custom format
userip-str	User IP address string
usermac-str	User MAC address string
uservid-str	User VID string
nasid-str	NAS device ID string
nasid2-str	NAS device ID string (supports 2 NAS ID)
acname-str	AC name string
apmac-str	Associated AP MAC address string
url-str	Original URL string
ssid-str	SSID string
port-str	Auth-Port string
ac-sno-str	SN string of the AC
ap-sno-str	SN string of the AP
md5	MD5 encryption
des	DES encryption
des_ecb	DES_ECB encryption
des_ecb3	DES_ECB3 encryption
none	Not-encrypted

Defaults The default URL redirection format is FS format.

Command Mode Template configuration mode

Usage Guide Use this command to set the URL redirection format based on the corresponding portal standard.

Configuration Examples N/A

Platform Description N/A

14.10 http redirect direct-arp

Use this command to set the address range of the authentication-exempted ARP.

Use the **no** form of this command to restore the default setting.

http redirect direct-arp { *ip-address* [*ip-mask*] }

no http redirect direct- arp { *ip-address* [*ip-mask*] }

Parameter Description

Parameter	**Description**
ip-address	IPv4 address
ip-mask	(Optional) IPv4 mask

Defaults No authentication-exempted ARP resource is configured by default.

Command Mode Global configuration mode

Usage Guide The user cannot learn the ARPs of devices such as the gateway with the ARP CHECK function enabled. Use this command to enable the device to learn the ARP within a specified IP address range without authentication.

Configuration Examples The following example sets the IP address 172.16.0.1 as the authentication-exempted ARP resource.

```
FS(config)# http redirect direct-arp 172.16.0.1
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

14.11 http redirect direct-site

Use this command to set the range of authentication-exempted network resources.

Use the **no** form of this command to restore the default setting.

http redirect direct-site { *ipv4-address* [*ip-mask*] [**arp**]| *mac-address* | range *starip-address endip-address*} [description *description-str*] [group *group-name*]

no http redirect direct-site { *ipv4-address* [*ip-mask*] | *mac-address* | range *startip-address endip-address* }

Parameter Description

Parameter	Description
ipv4-address	IPv4 address of the authentication-exempted network resources
ip-mask	IPv4 address mask of the authentication-exempted network resources (optional)
arp	If the ARP Check is enabled on the access device, the keyword arp is needed for ARP binding of the authentication-exempted network resources (optional). It is necessary for IPv4 network resources only.
mac-address	MAC address of the authentication-exempted user
startip-address	Start IP address of continuous authentication-exempted network resources.
endip-address	End IP address of continuous authentication-exempted network resources.
group-name	Group where authentication-exempted network resources belong.
description-str	Description of authentication-exempted network resources.

Defaults

No authentication-exempted network resource is set.

Command Mode

Global configuration mode

Usage Guide

When Web/802.1x authentication is enabled, all users must pass Web/client authentication to access network resources. This command is used to make certain network resources available to unauthenticated users. All users can access the authentication-exempted Web sites.

Up to 50 authentication-exempted users are supported.

Configuration Examples

The following example sets the Web site with IP address 172.16.0.1 as the authentication-exempted resource.

```
FS(config)# http redirect direct-site 172.16.0.1
```

The following example sets the Web site with MAC address 0000:5e00:0101 as the authentication-exempted resource.

```
FS(config)# http redirect direct-site 0000:5e00:0101
```

Related Commands

Command	Description
show http redirect	Displays the HTTP redirection configuration.

Platform Description

N/A

14.12 http redirect port

Use this command to redirect users' HTTP redirection request to a certain destination port.

Use the **no** form of this command to restore the default setting.

http redirect port *port-num*

no http redirect port *port-num*

Parameter Description

Parameter	**Description**
port-num	Destination port of the HTTP request

Defaults

The default is port 80.

Command Mode

Global configuration mode

Usage Guide

When you access the network resource, you send HTTP packets. The access device can intercept such HTTP packets to detect your access. If the access device detects that an unauthenticated user is accessing the network resource, it stops the users with an authentication page/client download page.

By default, the access device intercepts users' HTTP packets with port 80 to check whether they are accessing network resources.

This command is used to change the destination port of HTTP packets that are intercepted by the access device. Up to 10 ports can be configured, including port 80.

Configuration Examples

The following example redirects users' HTTP requests with port 8080.

```
FS(config)# http redirect port 8080
```

The following example does not redirect users' HTTP requests with port 80.

```
FS(config)# no http redirect port 80
```

Related Commands

Command	**Description**
show http redirect	Displays the HTTP redirection configuration.

Platform Description

N/A

14.13 http redirect session-limit

Use this command to set the total number of HTTP sessions that can be originated by an unauthenticated user, or the maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port.

Use the **no** form of this command to restore the default setting.

http redirect session-limit *session-num* [**port** *port-session-num*]

no http redirect session-limit

Parameter Description

Parameter	Description
session-num	Total number of HTTP sessions that can be originated by an unauthenticated user, in the range from 1 to 255.
port-session-num	The maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port, in the range from 1 to 65535.

Defaults

Totally 255 HTTP sessions can be originated by an unauthenticated user, and 300 HTTP sessions that can be originated by an unauthenticated user connected to each port.

Command Mode

Global configuration mode

Usage Guide

To prevent HTTP attacks caused by unauthenticated users from using up the TCP connections of the access device, the maximum number of HTTP sessions by unauthenticated users must be limited on the access device.

In addition to authentication, other programs may also occupy HTTP sessions. Therefore, it is not recommended that the maximum number of HTTP sessions by unauthenticated users be 1

Configuration Examples

The following example sets the maximum number of HTTP sessions originated by an unauthenticated user to 4.

```
FS(config)# http redirect session-limit 4
```

Related Commands

Command	Description
show http redirect	Displays the HTTP redirection configuration.

Platform Description

N/A

14.14 http redirect timeout

Use this command to set the timeout for the redirection connection maintenance.

Use the **no** form of this command to restore the default setting.

http redirect timeout *seconds*

no http redirect timeout

Parameter Description

Parameter	Description
seconds	Set the timeout for the redirection connection maintenance, in the range from 1 to 10 in the unit of seconds.

Defaults

The default is 3 seconds.

Command Mode

Global configuration mode

Usage Guide

This command is used to set the timeout for the redirection connection maintenance. After the three-way handshake succeeds, the redirection connection is maintained until the user sends an HTTP GET/HEAD packet and the system returns an HTTP redirection packet. This timeout is set to prevent users from occupying TCP connections for long without sending any GET/HEAD packets.

Configuration Examples

The following example sets the timeout for the redirection connection maintenance to 4 seconds.

```
FS(config)# http redirect timeout 4
```

Related Commands

Command	Description
show http redirect	Displays the HTTP redirection configuration.

Platform Description

N/A

14.15 ip

Use this command to set an IP address for the portal server.

Use the **no** form of this command to restore the default setting.

port { *ip-address* }

no port

Parameter Description

Parameter	Description
ip-address	The IPv4 address of the portal server

Defaults

No IP address is set for the portal server by default.

Command Mode

Template configuration mode

Usage Guide

This command takes place of the **http redirect** [*ip-address*] command, which is now hidden as a compatible command.

Configuration Examples

The following example sets the IP address of the eportalv1 template to 172.16.0.1.

```
FS(config.tmplt.eportalv1)#ip 172.16.0.1
FS(config.tmplt.eportalv1)#
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

14.16 ip portal source-interface

Use this command to specify a communication port for the portal server.

Use the **no** form of this command to restore the default setting.

ip portal source-interface *interface-type interface-num*

no ip portal source-interface

Parameter Description

Parameter	Description
interface-type	Port type
interface-num	Port No.

Defaults No communication interface is specified by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example specifies an aggregate port as the communication port.

```
FS (config)# ip portal source-interface Aggregateport 1
```

Platform Description N/A

14.17 iportal nat enable

Use this command to enable NAT function for local Web authentication.

Use the **no** form of this command to restore the default setting.

iportal nat enable

no iportal nat enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults NAT is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

The following example enables NAT function for local Web authentication.

```
FS (config)# iportal nat enable
```

Platform Description

N/A

14.18 iportal retransmit

Use this command to set the retransmission count of HTTP packets.

Use the **no** form of this command to restore the default setting.

iportal retransmit *times*

no iportal retransmit

Parameter Description

Parameter	Description
times	Retransmission count

Defaults

The retransmission count of HTTP packets is 3 by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the retransmission count of HTTP packets to 5.

```
FS (config)# iportal retransmit 5
```

Platform Description

N/A

14.19 iportal service

Use this command to configure a service template.

Use the **no** form of this command to restore the default setting.

iportal service [internet *internet-name*] **[local** *local-name* **]**

no iportal service [internet *internet-name*] **[local** *local-name* **]**

Parameter Description

Parameter	Description
internet-name	External service name
local-name	Local service name

Defaults

No service template is configured by default.

Command

Global configuration mode

Mode

Usage Guide N/A

Configuration Examples The following example configures a local service template.

```
FS (config)# iportal service local local-srv
```

Platform Description N/A

14.20 iportal user-agent

Use this command to configure the name and string for User Agent (UA).

Use the **no** form of this command to remove the UA name and string.

iportal user-agent *ua-name* **type mobile** *ua-string*

no iportal user-agent *ua-name* **type mobile** *ua-string*

Parameter Description

Parameter	Description
ua-name	UA name
ua-string	UA string

Defaults No UA name and string is configured by default.

Command Mode Global configuration mode

Usage Guide Terminal recognition is used to replace this command at present.

Configuration Examples

Platform Description N/A

14.21 login-popup

Use this command to configure a pre-login popup advertisement.

Use the **no** form of this command to restore the default setting.

login-popup *url-string*

no login-popup

Parameter Description

Parameter	Description

url-string	Ad URL

Defaults

No pre-login popup advertisement is configured by default.

Command Mode

Template configuration mode

Usage Guide

The URL of the popup advertisement should begin with "http://" or "https://".

Configuration Examples

The following example configures a pre-login popup advertisement.

```
FS(config.tmplt.iportal)#login-popup http://www.FS.com.cn
```

Platform Description

N/A

14.22 online-popup

Use this command to configure a post-login popup advertisement.

Use the no form of this command to restore the default setting.

online-popup *url-string*

no online-popup

Parameter Description

Parameter	Description
url-string	Ad URL

Defaults

No post-login popup advertisement is configured by default.

Command Mode

Template configuration mode

Usage Guide

The URL of the popup advertisement should begin with "http://" or "https://".

Configuration Examples

The following example configures a post-login popup advertisement.

```
FS(config.tmplt.iportal)#online-popup http://www.FS.com.cn
```

Platform Description

N/A

14.23 page-suite

Use this command to configure a resource suite for the login page.

Use the **no** form of this command to restore the default setting.

page-suite *filename*

no page-suite

Parameter Description

Parameter	Description
filename	Resource suite name

Defaults The installed resource suite is used by default.

Command Mode Template configuration mode

Usage Guide Make sure to download page resource files in the directory of portal/zip under FLASH before.

Configuration Examples The following example configures a page suite for internal Web authentication.

```
FS(config.tmplt.iportal)#page-suite FSpage
```

Platform Description N/A

14.24 port

Use this command to set a surveillance port for the portal server.

Use the **no** form of this command to restore the default setting.

port { *port-num* }

no port

Parameter Description

Parameter	Description
port	The surveillance port of the portal server, which is on only the 2nd generation portal server,

Defaults The default is 50100 based on the UDP protocol.

Command Mode Template configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.25 redirect

Use this command to set the redirect packet protocol.

Use the **no** form of this command to restore the default setting.

redirect { *http* | *js* }

no redirect

Parameter Description

Parameter	Description
http	HTTP 302
js	HTTP 200

Defaults The default is HTTP 200.

Command Mode Template configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.26 show web-auth cgi

Use this command to display CGI configuration.

show web-auth cgi

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays CGI configuration,

```
FS# show web-auth cgi
Total 0 cgi items:
id-string                url-string
---------------     -----------------------------------
```

Platform Description

N/A

14.27 show web-auth control

Use this command to display the authentication configuration.

show web-auth control

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the authentication configuration and statistics information on the interface.

```
FS(config)#show web-auth control
 Port                              Control   Server Name              Online User Count
 ------------------------- -------- --------------------- -----------------
 GigabitEthernet 0/1          On          <not configured>         0
FS(config)#
```

Field	Description
Port	Name of the authentication port.
Control	Displays whether the Web authentication is enabled on the port or not.
Server Name	The customized server name on the port. **<not configured>** indicates the server name has not been configured.
Online User Count	The number of online users on this port.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.28 show web-auth direct-arp

Use this command to display the address range of the authentication-exempted ARP.

show web-auth direct-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

I N/A

Configuration Examples

The following example displays the address range of the authentication-exempted ARP.

```
FS(config)#show web-auth direct-arp
Direct arps:
   Address              Mask
   --------------- ---------------
   1.1.1.1            255.255.255.255
   2.2.2.2            255.255.255.255
FS(config)#
```

Field	Description
Address	IPv4 address.
Mask	IPv4 mask.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.29 show web-auth direct-host

This command is used to display the Web authentication-exempted users.

show web-auth direct-host

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the Web authentication-exempted users.

```
FS# show web-auth direct-host
Direct hosts:
   Address                  Mask                      Port              ARP Binding
   ---------------- ---------------- ---------- ------------
   192.168.0.1          255.255.255.255     Fa0/2            On
   192.168.4.11         255.255.255.255     Fa0/10           On
   192.168.5.0          255.255.255.0         Fa0/16           Off
```

Field	Description
Address	IP address of the user free of authentication
Mask	IP address mask of the user free of authentication
Port	Access device port that is bound with the user’s IP address
ARP Binding	Enable/Disable ARP binding

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.30 show web-auth direct site

Use this command to display the range of the Web authentication-exempted network resources.

show web-auth direct-site

Parameter Description

Parameter	Description

N/A	N/A

Defaults No network resource without authentication is set.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the range of the Web authentication-exempted network resources without authentication.

```
FS(config)#show web-auth direct-site
Direct sites:
  Address          Mask             ARP Binding
  --------------- --------------- -----------
  1.1.1.1          255.255.255.255 Off
  2.2.2.2          255.255.255.255 On
FS(config)#
```

Field	Description
Address	IP address.
Mask	IP mask.
ARP Binding	Displays whether the ARP binding function is enabled.

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

14.31 show web-auth global

Use this command to display global Web authentication configuration.

show web-auth global

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays global WEB authentication configuration.

```
FS# show web-auth parameter
Webauth..........................................enable
Webauth-type.....................................external
Customized-pages.................................(Not Configured)
Server-port......................................8081
Public account...................................disable
Authentication...................................(Not Configured)
Current global template:
      name:........................................eportalv1
      type:........................................v1
      Ip:..........................................192.168.197.79
      URL:.........................................http://192.168.197.79:8080/eportal/index.jsp
```

Field	Description
Webauth-type	Web authentication type
Customized-pages	The custom page of local Web authentication
Server-port	The surveillance port of local Web authentication
Public account	Whether the public account is enabled
Authentication	Authentication method
Current global template	Current global template

Platform Description N/A

14.32 show web-auth global authentication

Use this command to display the Web authentication method.

show web-auth global authentication

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the WEB authentication method.

Examples

```
FS# show web-auth global authentication
Webauth...........................................enable
Authentication....................................(Not Configured)
```

Field	Description
Webauth	Whether Web authentication is enabled
Authentication	Authentication method

Platform Description N/A

14.33 show web-auth global customized-pages

Use this command to display the customized page information.

show web-auth global customized-pages

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the customized page information.

```
FS# show web-auth global customized-pages
Webauth...........................................enable
Customized-pages..................................(Not Configured)
```

Platform Description N/A

14.34 show web-auth global local-portal

Use this command to display the local portal server configuration.

show web-auth global local-portal

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the local portal server configuration.

```
FS# show web-auth global local-portal
Webauth..........................................enable
Server-port......................................8081
Public account...................................disable
```

Field	Description
Webauth	Whether Web authentication is enabled
Server-port	Surveillance port
Public account	Whether the public account is enabled

Platform Description N/A

14.35 show web-auth global template

Use this command to display the global authentication template.

show web-auth global template

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the global authentication template.

```
FS# show web-auth global template
Webauth..........................................enable
Current global template:
     name:.......................................eportalv1
     type:.......................................v1
     Ip:.........................................192.168.197.79
     URL:........................................http://192.168.197.79:8080/eportal/index.jsp
```

Field	Description
Webauth	WEB authentication is enabled.
Current global template	Current global template summary

Platform Description N/A

14.36 show web-auth global webauth-type

Use this command to display the global authentication type.

show web-auth global webauth-type

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the global authentication type.

```
FS# show web-auth global webauth-type
Webauth..........................................enable
Webauth-type.....................................external
```

Field	Description
Webauth	Whether Web authentication is enabled
Webauth-type	Authentication type

Platform Description N/A

14.37 show web-auth info

Use this command to display user authentication configuration.

show web-auth info

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays user authentication configuration.

```
FS# show web-auth cgi
web-auth info:
    Update interval: 180
    User mode: ip
    Portal key: FS
```

Field	Description
Update interval	Update interval of user information
User mode	User binding mode
Portal key	Portal communication key

Platform Description

N/A

14.38 show web-auth ip-mapping

Use this command to display the portal-client mapping rule.

show web-auth ip-mapping

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the portal-client mapping rule.

```
FS(config)#show web-auth ip-mapping
------------------------------------------------------------
  Name:           iportal
  Ip:             0.0.0.0
  Url:
  Ip-Mapping:
------------------------------------------------------------
  Name:           eportalv1
  Ip:             172.18.105.9
  Url:            http://172.18.105.9:8080/eportal/index.jsp
  Ip-Mapping:
                  1.1.1.0-255.255.255.0              Global
FS(config)#
```

Platform

N/A

Description

14.39 show web-auth local-portal

Use this command to display local portal server configuration.

show web-auth local-portal

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays local portal server configuration.

```
FS# show web-auth local-portal
Local web-auth info:
    Server-port:                    8081
    AAA method-list:                 (Not Configured)
    Public account:                 disable
```

Field	Description
Server-port	Surveillance port
AAA method-list	AAA method list
Public account	Whether the public account is enabled

Platform Description

N/A

14.40 show web-auth parameter

Use this command to display the HTTP redirect configuration.

show web-auth parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the HTTP redirect configuration

```
FS# show web-auth parameter
  session-limit: 10
  timeout:              5
```

Field	Description
session-limit	Total number of HTTP sessions that are created by an unauthenticated user.
timeout	Timeout interval of the redirection connection.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.41 show web-auth portal-check

Use this command to display the portal-check configuration.

show web-auth portal-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the portal-check configuration.

```
FS#sh web portal-check
Check:              Enable
  Interval:       3s
  Timeout:         5s
  Retransmit:   3
Escape:              Enable
Nokick:              Disable
```

Platform Description N/A

14.42 show web-auth rdport

Use this command to display the TCP interception port.

show web-auth rdport

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the TCP interception port.

```
FS#show web-auth rdport
Rd-Port:
80 443
FS#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.43 show web-auth syslog ip

Use this command to display online and offline records about users.

show web-auth syslog ip *ip-address*

Parameter Description

Parameter	Description
ip-address	User’s IP address

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays online and offline records about users.

```
FS#show web-auth syslog ip 192.168.197.35
Address: 192.168.197.35     Core-index 0 Current index 2
Index:                    0
 Time:                     2015-10-16 20:37:34
 Behavior:                ONLINE
 Mac:                      00d0.f822.33e7
 Vid:                     101
 Port:                    Gi3/1
 Timeused:                 0d 00:00:00
 Flow_up:                  0
 Flow_down:                 0

 Index:                   1
 Time:                     2015-10-16 20:42:08
 Behavior:                OFFLINE
 Mac:                      00d0.f822.33e7
 Vid:                     101
 Port:                    Gi3/1
 Timeused:                 0d 00:04:27
 Flow_up:                  2107872
 Flow_down:                 2108224
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.44 show web-auth template

Use this command to display the portal server configuration.

show web-auth template

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the portal server configuration.

Configuration Examples

The following example displays the port server configuration.

```
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
```

Field	Description
Name	Template name.
Url	Server homepage address.
Ip	Server IP address.
Type	Server type, including the first generation portal server v1, the second generation portal server v2 and the intra portal server intra.
Port	The protocol packet communication port of the server, which is on only the second generation portal server.
Acctmlist	Accounting method list name, which is on only the second generation portal server and the intra portal server
Authmlist	Authentication method list name. which is on only the second generation portal server and the intra portal server

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.45 show web-auth user

Use this comma to display the online information, including IP address, interface, and online duration, of all users or the specified users.

show web-auth user { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* | **escape** }

Parameter Description

Parameter	Description
ip-address	IPv4 address of the user.

mac-address	MAC address of the user.
name-string	User name.
num	AAA session ID.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the global Web authentication configuration and statistics.

```
FS# show web-auth user all
Current user num :    4, online 2

Address                  Online     Time Limit         Time Used        Status    Name
--------------- -------    ------------- -------------- -------- ---------
192.168.0.11       On           0d 01:00:00     0d 00:15:10       Active
192.168.0.13       On           0d 01:00:00     0d 00:00:59       Active     111
192.168.0.25       Off         0d 01:00:00     0d 00:00:59       Create
192.168.0.46       Off         0d 01:00:00     0d 01:00:00       Destroy    222

FS# show web-auth user ip 192.168.0.11
Address             :      192.168.0.11
 Mac                     :      00d0.f800.2233
 Port                   :      Gi0/2
 Online               :      On
 Time Limit      :      0d 01:00:00
 Time Used        :      0d 00:15:10
 Time Start       :      2009-02-22 20:05:10
 Status               :      Active
```

Field	**Description**
Address	IP address of the user
Mac	MAC address of the user
Port	Access device port connected to the user
Online	Whether the user is online
Time Limit	Available duration of the user. 0 means unlimited.
Time Used	Online duration of the user
Time Start	Time when the user passes authentication and gets online
Status	User status. Active means the user is normally online, Create means the user is created without any settings, Destroy means the user is deleted with its settings not cleared.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.46 time-interval

Use this command to set the interval for popup advertisement.

Use the **no** form of this command to restore the default setting.

time-interval *{ hour }*

no time-interval

Parameter Description

Parameter	Description
hour	The popup interval in the range from 0 to 24 in the unit of hours

Defaults

The default is 1 hour.

Command Mode

Template configuration mode

Usage Guide

If the parameter hour is 0, it means no popup interval.

Configuration Examples

The following example sets the interval for popup advertisement to 2 hours.

```
FS(config.tmplt.iportal)#time-interval 2
```

Platform Description

N/A

14.47 url

Use this command to set the portal server URL.

Use the **no** form of this command to restore the default setting.

url *url-string*

no url

Parameter Description

Parameter	Description
url-string	Portal server URL, starting with **http://** or **https://**. The maximum length of this address is 255 bytes.

Defaults

No portal server URL is set by default.

Command Mode

Template configuration mode

Usage Guide

This command takes place of the **http redirect homepage** [*url-string*] command, which is now hidden as a compatible command.,

If no URL is specified, the default URL in the **http://[ip-address]** format will be adopted, among which **ip-address** is the IP address of the server.

Configuration Examples

The following example sets the eportalv1 template URL to **http://www.web-auth.net/login**.

```
FS(config.tmplt.eportalv1)#url http://www.web-auth.net/login
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.48 web-auth account-share ip-limit

Use this command to set the account share limit.

Use the **no** form of this command to remove the settings.

web-auth account-share ip-limit { *limit-num* }

no web-auth account-share

Parameter Description

Parameter	Description
limit-num	The account share limit

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the account share limit to 20.

```
FS (config)# web-auth account-share ip-limit 20
```

Platform Description

14.49 web-auth acl

Use this command to configure a blacklist or whitelist.

Use **no** form of this command to restore the default setting.

web-auth acl { **black-ip** *ip*|**black-port** *port* | **black-url** *name* | **white-url** *name* }

no web-auth acl { **black-ip** *ip* | **black-port** *port* **|** **black-url** *name* **|** **white-url** *name* }

Parameter Description

Parameter	Description
ip	Blacklist /Whitelist IP address
port	Blacklist /Whitelist Port number in the range from 1 to 65535
name	Blacklist /Whitelist URL

Defaults N/A

Command Mode Global configuration mode/WLAN security configuration mode

Usage Guide The whitelist allows listed users to access specific network resources before authentication.

The blacklist prohibits listed users from accessing specific network resources after authentication.

Configuration Examples N/A

Platform Description N/A

14.50 web-auth customized-logo enable

Use this command to enable the custom logo on the authentication page.

Use **no** form of this command to remove the customized logo.

web-auth customized-logo enable

no web-auth customized-logo

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables the custom logo on the authentication page.

```
FS (config)# web customized-logo enable
```

Platform Description N/A

14.51 web-auth direct-host

Use this command to set the authentication-exempted IP/MAC address range.

Use the **no** form of this command to restore the default setting.

web-auth direct-host { *ipv4-address* [i*p-mask*] [**arp**] | *mac-address* | range *starip-address endip-address* } [**port** *interface-name*] [description *description-str*] [group *group-name*]

no web-auth direct-host { *ipv4-address* [i*p-mask*] | *mac-address* | range *starip-address endip-address* }

Parameter Description

Parameter	Description
ip-address	IPv4 address of authentication-exempted user
ip-mask	Mask of the IPv4 address free of authentication (optional).
port *interface-name*	Binds user's IP address with a port of the access device (optional).
arp	If ARP CHECK is enabled on the access device, keyword arp is needed for ARP binding of the IP address used by users free of authentication (optional). It is necessary for IPv4 addresses only.
mac-address	MAC address of authentication-exempted user
startip-address	Start IP address of continuous authentication-exempted network resources.
endip-address	End IP address of continuous authentication-exempted network resources.
group-name	Group where authentication-exempted network resources belong.
description-str	Description of authentication-exempted network resources.

Defaults No user is exempted from authentication. All users must pass the Web authentication to access the restricted network resources.

Command Mode Global configuration mode

Usage Guide When a user is set to be exempted from authentication, it can access all reachable network resources without Web authentication.

Up to 50 users can be set to be exempted from authentication.

Configuration Examples The following example sets the user with the IP address 172.16.0.1 to be exempted from authentication.

```
FS(config)# web-auth direct-host 172.16.0.1
```

The following example sets the user with the MAC address 0000:5e00:0101 to be exempted from authentication.

```
FS(config)# web-auth direct-host 0000:5e00:0101
```

Related Commands

Command	Description

show web-auth direct-host	Displays the users free of Web authentication.

Platform Description N/A

14.52 web-auth enable

Use this command to enable the Web authentication function on a port. This command is compatible with the **web-auth port-control** command.

Use the **no** form of this command to restore the default setting.

web-auth enable

no web-auth enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The Web authentication function is disabled on the port by default.

The **default** template is eportalv1.

Command Mode Interface configuration mode

Usage Guide To ensure the Web authentication function, the authentication page URL should be configured.

Because template applications are integrated into the controlled switch, the template or the server applications of the interface where the Web authentication function is disabled will be automatically cleared. This command is compatible with the original command that used to apply the template or server application in the global configuration mode.

Configuration Examples The following example enables the Web authentication function on gigabitEthernet 0/14.

```
FS(config)# interface GigabitEthernet 0/14
FS(config-if-GigabitEthernet 0/14)# web-auth enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

14.53 web-auth group

Use this command to configure group information.

Use the **no** form of this command to remove the configuration.

web-auth group *group-name* [description *description-str*]

no web-auth group ***group-name***

Parameter Description

Parameter	**Description**
group-name	Group name
description-str	Description of the group

Defaults By default, no accounting-exempted IP address is configured.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures group information.

```
FS (config)# web-auth group group-1 [description DESC]
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

14.54 web-auth logging enable

Use this command to enable the Web authentication syslog function.

Use the **no** form of this command to restore the default setting.

web-auth logging enable { *num* }

no web-auth logging enable

Parameter Description

Parameter	**Description**
num	The syslog printing rate, indicating how many syslog entries can be printed in a second. The value is in the range from 0 to 65535. 0 indicates no limit.

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This command is used to limit the syslog printing rate for only the functional module.

Configuration The following example enables the syslog printing with no rate limit.

Examples

```
FS(config)# web-auth logging enable 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.55 web-auth portal key

Use this command to set the communication key between the access device and the authentication server.

Use the **no** form of this command to clear the communication key between the redirected Web request of a user and the authentication server.

web-auth portal key *key-string*

no web-auth portal key

Parameter Description

Parameter	Description
key-string	Communication key between the access device and the authentication server. The maximum length of the key is 255 bytes.

Defaults

No key is set by default.

Command Mode

Global configuration mode

Usage Guide

To use the Web authentication function, the communication key between the access device and the authentication server must be set.

Configuration Examples

The following example sets the communication key between the access device and the authentication server to web-auth.

```
FS(config)# web-auth portal key web-auth
```

Related Commands

Command	Description
http redirect	Sets the IP address of the authentication server.
http redirect homepage	Sets the address of the authentication homepage.
web-auth port-control	Enables the Web authentication on the port.

Platform Description

N/A

14.56 web-auth portal-check

Use this command to enable portal server check.

Use the **no** form of this command to restore the default setting.

web-auth portal-check [**interval** *intsec*] [**timeout** *tosec*] [**retransmit** *retires*]

no web-auth porta-check

Parameter Description

Parameter	Description
Intsec	Check interval in the range from 1 to 1,000 in the unit of seconds. The default is 10 seconds.
tosec	Timeout interval in the range from 1 to 1,000 in the unit of seconds. The default is 5 seconds.
retries	Retry count in the range from 1 to 100. The default is 3.

Defaults Portal server check is disabled by default.

Command Mode Global configuration mode

Usage Guide It is recommended to use this command when there are multiple servers.

Configuration Examples The following example enables portal server check.

```
FS (config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

Platform Description N/A

14.57 web-auth template

Use this command to create the first generation authentication template and enter its configuration mode.

web-auth template eportalv1

Use this command to create the customized authentication template and enter its configuration mode.

web-auth template { template-name } **v1**

Use this command to create the second generation authentication template and enter its configuration mode.

web-auth template eportalv2

Use this command to create the customized second generation authentication template and enter its configuration mode.

web-auth template { *template-name* } **v2**

Use this command to remove the template.

no web-auth template { *template-name* }

Parameter Description

Parameter	Description
eportalv1	Applies the first generation authentication template.
eportalv2	Applies the second generation authentication template.
iportal	Applies the built-in authentication template.
template-name	Sets the name of the customized authentication template.

Defaults

No template is configured by default.

Command Mode

Global configuration mode

Usage Guide

You can enter the **eportalv1** template mode to configure the IP address and URL instead of executing the **http redirect** and **http redirect homepage** commands**.** The **http redirect** and **http redirect homepage** commands are compatible on the device, which will be converted to this command.

The original command **portal-server** is compatible on the device, which will be converted to this command.

To ensure the Web authentication function, configure and apply a functional portal server. The **eportalv1** template is applied by default. The IP address, the URL and the communication secret key of the **eportalv1** template should be configured. If no URL format is specified, the default **http://[ip-address]** format will be adopted. The IP address of the portal server is the network resource exempted from authentication, so the unauthenticated user can access it. The device limits the uplink traffic that accesses the IP address to prevent attacks. The upper limit is proportionate to the number of the physical ports.

Configuration Examples

The following example configures the **eportalv1** template.

```
FS(config)# web-auth template eportalv1
FS(config.tmplt.eportalv1)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.58 web-auth update-interval

Use this command to set the interval at which the online user information is updated.

Use the **no** form of this command to restore the default setting.

web-auth update-interval {*seconds*}

no web-auth update-interval

Parameter Description

Parameter	Description

seconds	Update interval in seconds, in the range from 30 to 3,600 in the unit of seconds.

Defaults

The default is 180 seconds.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the interval at which the online user information is updated to 60 seconds.

```
FS(config)# web-auth update-interval 60
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15 Global IP-MAC Binding Commands

15.1 address-bind

Use this command to configure global IP-MAC address binding. Use the **no** form of this command to restore the default setting.

address-bind { *ip-address* | *ipv6-address* }   mac-address

no address-bind { *ip-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ip-address	IPv4 address to be bound
ipv6-address	IPv6 address to be bound
mac-address	MAC address to be bound

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

```
The following example configures global IP-MAC address binding.FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# address-bind 192.168.5.1 00d0.f800.0001
```

Related Commands

Command	Description
show address-bind	Displays the IP address-MAC address binding table.

Platform Description

N/A

15.2 address-bind binding-filter logging

Use this command to enable the logging filter. Use the **no** form of this command to restore the default setting.

address-bind binding-filter logging [**rate-limit** *rate*]

no address-bind binding-filter logging

Parameter Description

Parameter	Description
rate-limit ***rate***	Printing rate of the logging filter of global IPv4 MAC binding. By default, the rate is 10 logs per minute. The configurable range is from 1 to 120 logs per minute.

Defaults

Logging filter is disabled.

Command Mode

Global configuration mode

Usage Guide

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 Examples

The following example enables logging filter:

```
FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# address-bind binding-filter logging
FS(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.3 address-bind install

Use this command to enable a binding policy globally. Use the **no** form of this command to restore the default setting.

address-bind install

no address-bind install

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If you bind an IP address to a MAC address, run this command to make the installation policy take effect.

Configuration Examples

The following example binds an IP address to a MAC address globally.

```
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
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.4 address-bind ipv6-mode

This command is used to set the IPv6 address binding mode. Use the **no** form of this command to restore the default setting.

This command is also used to set the compatible mode.

address-bind ipv6-mode { **compatible** | **loose** | **strict** }

no address-bind ipv6-mode

Parameter Description

Parameter	Description
compatible	Compatible mode
loose	Loose mode
strict	Strict mode

Defaults The default is strict mode.

Command Mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the IPv6 address binding mode.

```
FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# address-bind ipv6-mode compatible
```

Related Commands

Command	Description
show address-bind uplink	Displays the exceptional port of the address binding.

Platform Description N/A

15.5 address-bind uplink

This command is used to configure the exception port. Use the **no** form of this command to restore the default setting.

address-bind uplink *interface-id*

no address-bind uplink *interface-id*

Parameter

Parameter	Description

Description

interface-id	Switching port or layer 2 aggregate port.

Defaults

All ports are non-exception ports by default.

Command Mode

Global configuration mode.

Usage Guide

If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.

Configuration Examples

```
The following example configures the exception port. FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
FS(config)# address-bind uplink GigabitEthernet 0/1
```

Related Commands

Command	Description
show address-bind uplink	Displays the exceptional port of address binding.

Platform Description

N/A

15.6 show address-bind

Use this command to display global IP address-MAC address binding.

show address-bind

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following example displays global IPv4 address-MAC address binding.

```
FS#show address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
---------------     ----------------
192.168.5.1         00d0.f800.0001
```

Field	Description
Total Bind Addresses in System	IPv4 address-MAC address binding count

IP Address	Bound IP address
Binding MAC Addr	Bound MAC address

Related Commands

Command	Description
address-bind	Enables IP address-MAC address binding.

Platform Description

N/A

15.7 show address-bind uplink

Use this command to display the exception port.

show address-bind uplink

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

N/A

Usage Guide

N/A

Configuration Examples

The following example displays the exception port.

```
FS#show address-bind uplink
Port        State
---------- ---------
Gi0/1       Enabled
Default     Disabled
```

Field	Description
Port	Short for exception ports. All ports are non-exception ports by default.
State	Indicates whether the port is exception port. State Enabled indicates that it is an exception port while state Disabled indicates that it it not.

Related Commands

Command	Description
address-bind uplink	Sets the exception port.

Platform Description

N/A

16 IPoE Commands

16.1 clear ipoe-auth user

Use this command to clear IPv4 IPoE authenticated clients by forcing them to go offline.

clear ipoe-auth user { **all** | **ip** *ip-address* | **mac** *mac-address* }

Parameter Description

Parameter	Description
ip-address	Specifies the IP address.
mac-address	Specifies the source MAC address.

Defaults IPv4 IPoE authenticated clients are not cleared by default.

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear IPv4 IPoE authenticated clients by forcing them to go offline.

Configuration Example #Clear all IPv4 IPoE authenticated clients.

```
FS# clear ipoe-auth user all
```

Verification Verify that no user entry is displayed after running the **show ipoe-auth summary** command.

16.2 ipoe-auth enable

Use this command to enable the IPv4 IPoE function.

ipoe-auth enable

Use the **no** form of this command to disable the IPv4 IPoE function.

no ipoe-auth enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The IPv4 IPoE function is disabled by default.

Command Mode Global configuration mode

Usage Guide Other IPv4 IPoE-related configurations can take effect only after the IPv4 IPoE function is enabled.

Configuration Example #Enable the IPv4 IPoE function.

```
FS#configure
```

```
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# ipoe-auth enable
```

Verification Run the **show running-config** command to display the configuration result.

16.3 ipoe-auth quiet-period

Use this command to configure the silent time for IPv4 IPoE authenticated clients.

ipoe-auth quiet-period *time*

Use the **no** form of this command to restore the default silent time.

no ipoe-auth quiet-period

Parameter Description

Parameter	Description
time	Specifies the silent time. The value range is from 0 to 65,535 seconds. No input is equivalent to the value 10 by default.

Defaults The silent time of IPv4 IPoE authenticated clients is 10 seconds by default.

Command Mode Global configuration mode

Usage Guide Use this command to set the silent time of a client upon 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. After the silent time, if the device receives packets from the client again, the device can authenticate the client.

Configuration Example #Configure the silent time of IPv4 IPoE authenticated client to 100 seconds in global configuration mode.

```
FS#configure
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# ipoe-auth quiet-period 100
```

Verification Run the **show running-config** command to display the configuration result.

16.4 ipoe-auth server-timeout

Use this command to configure the IPv4 IPoE authentication timeout period.

ipoe-auth server-timeout *time*

Use the **no** form of this command to restore the default authentication timeout period.

no ipoe-auth server-timeout

Parameter

Parameter	Description

Description

time	Specifies the authentication timeout period. The value range is from 1 to 65,535 seconds. No input is equivalent to the value 30 by default.

Defaults The IPv4 IPoE authentication timeout period is 30 seconds by default.

Command Mode Global configuration mode

Usage Guide Use this command to ensure that the IPv4 IPoE timeout period is longer than timeout period of the RADIUS server.

Configuration Example #Configure the IPv4 IPoE authentication timeout period to 30 seconds in global configuration mode.

```
FS#configure
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# ipoe-auth server-timeout 100
```

Verification Run the **show running-config** command to display the configuration result.

16.5 ipoe-auth user-limit

Use this command to configure the maximum number of IPv4 IPoE authenticated clients allowed.

ipoe-auth user-limit *number*

Use the **no** form of this command to restore the default maximum number of IPv4 IPoE authenticated clients allowed.

no ipoe-auth user-limit

Parameter Description

Parameter	**Description**
number	Specifies the maximum number of IPv4 IPoE authenticated clients. The value range is from 1 to 1,000,000. No input is equivalent to the value 0 by default, and indicates that the maximum number is not limited.

Defaults The number of IPv4 IPoE authenticated clients is not limited by default.

Command Mode Global configuration mode

Usage Guide When the number of IPv4 IPoE authenticated clients reaches the maximum value, no other clients can perform IPoE authentication after they go online.

Configuration Example #Configure the maximum number of IPv4 IPoE authenticated clients allowed to 100.

```
FS#configure
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# ipoe-auth user-limit 100
```

Verification Run the **show running-config** command to display the configuration result.

16.6 show ipoe-auth summary

Use this command to display information related to an IPv4 IPoE authenticated client.

show ipoe-auth summary

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide Use this command to display the statistics of IPv4 IPoE authenticated clients.

Configuration Example

#Display the statistics of IPv4 IPoE authenticated clients in privileged EXEC mode.

```
FS#show ipoe-authe summary
ID          User          MAC                 Interface VLAN INNER-VLAN Auth-State          Backend-State Port-Status
User-Type Time
-------- ---------- --------------    --------- ---- ---------- --------------- ------------- ----------- --------- ------------------
```

Field description:

Field	Description
ID	ID obtained from the AAA server by running the **show aaa user all** command
User	Username
MAC Address	MAC address of the authenticated client
Interface	Interface of the authenticated client
VLAN	ID of the VLAN where the authenticated client is located
INNER-VLAN	ID of the inner VLAN where the authenticated client is located. This field is supported b the device supporting two layers of tags of the authenticated client.
Auth-State	Front-end authentication status
Backend-State	Back-end authentication status
Port-State	Authentication status of the port
User-Type	Authentication type
Time	Online duration

16.7 show ipoe-auth user

Use this command to display information about the IPv4 IPoE authenticated client.

show ipoe-auth user [**mac** *mac-address*] [**username** *name*]

Parameter Description

Parameter	Description
mac-address	Source MAC address
name	Username

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide Use this command to display information about the IPv4 IPoE authenticated client.

Configuration Example #Display information about the IPv4 IPoE authenticated client in privileged EXEC mode.

```
FS# show ipoe-auth user mac 0000.0000.0001
User name: 000000000001
User id: 150994945
Type: static
Mac address is 0000.0000.0001
Vlan id is 10
Access from port Gi4/8
Time online: 0days 0h 0m20s
User ip address is 192.168.197.159
Max user number on this port is 10
Authorization session time is 20736000 seconds
Start accounting
```

Field description:

Field	Description
User name	Username
Type	User type
Mac address	MAC address of a user
Vlan id	VLAN ID of a user
Access from port	Port where the client is located
Time online	Online duration of a user
User ip address	IP address of a user
Max user number on this port	Maximum number of users on a port
Authorization session time	Authorization session time of a client

17 IP Group Commands

17.1 description

Configure IP address group description.

description [*name*]

Delete IP address group description.

no description

Parameter Description

Parameter	Description
name	Descriptive string, which can consist of up to 32 characters (spaces are not allowed)

Defaults By default, no descriptive string is configured.

Command Mode IP address group configuration mode

Default Level 14

Usage Guide N/A

Configuration Example 1. Configure IP address group description.

```
FS(config-ip-group)#description test
```

2. Delete IP address group description.

```
FS(config-ip-group)#no description
```

Verification Run the **show ip-group** [*id*] command to display IP address group configurations.

17.2 ip-group

Configure an IP address group.

ip-group *id*

Delete an IP address group.

no ip-group *id*

Parameter Description

Parameter	Description
id	IP address group index, which ranges from 1 to 1,000

Defaults By default, no IP address group is configured.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Example

1. Configure an IP address group.

```
FS(config)#ip-group 1
```

2. Delete an IP address group.

```
FS(config)# no ip-group 1
```

Verification Run the **show ip-group** [*id*] command to display IP address group configurations.

17.3 ip-range

Configure an IP address range.

ip-range *start* [*end*]

Delete an IP address range.

no ip-range *start* [*end*]

Parameter Description

Parameter	Description
start	Start address of the IP address range
end	End address of the IP address range (if **end** is not set, it uses the value of **start** by default)

Defaults By default, no IP address range is configured.

Command Mode IP address group configuration mode

Default Level 14

Usage Guide N/A

Configuration Example

1. Configure the IP address range 1.1.1.1–1.1.1.10.

```
FS(config-ip-group)#p-range 1.1.1.2 1.1.1.10
```

2. Delete the IP address range 1.1.1.1–1.1.1.10.

```
FS(config-ip-group)#noip-range 1.1.1.2 1.1.1.10
```

Verification Run the **show ip-group** [*id*] command to display IP address group configurations.

17.4 ip-subnet

Configure an IP network segment.

ip-subnet *subnet {mask | mask_len }*

Delete an IP network segment.

no ip-subnet *subnet mask_len*

Parameter Description

Parameter	Description
subnet	Start address of the IP network segment
mask	Mask
mask_len	Mask length

Defaults By default, no IP network segment is configured.

Command Mode IP address group configuration mode

Default Level 14

Usage Guide N/A

Configuration Example 1. Configure an IP network segment.

```
FS(config-ip-group)#ip-subnet 10.10.10.0 24
```

2. Delete an IP network segment.

```
FS(config-ip-group)#noip-subnet 10.10.10.0 24
```

Verification Run the **show ip-group** [*id*] command to display IP address group configurations.

17.5 route-db

Configure a routing address database.

route-db *name*

Delete a routing address database.

no route-db *name*

Parameter Description

Parameter	Description
name	Name of a routing address database list.

Defaults By default, no routing address database is configured.

Command Mode IP address group configuration mode

Usage Guide N/A

Configuration Example

1. Configure an IP address segment.

```
FS(config-ip-group)#route-db cmc
```

2. Delete an IP address segment.

```
FS(config-ip-group)#no route-db cmc
```

Verification Run the **show ip-group** [*id*] command to display the configuration information of an IP group.

17.6 show ip-group

Display IP address group configurations.

show ip-group [*id*]

Parameter Description

Parameter	Description
id	ID of an IP address group

Command Mode Privileged mode, global configuration mode, or interface configuration mode

Default Level 14

Default Level If the **id** parameter is set, the configurations of the corresponding IP address group are displayed. If the **id** parameter is not set, the configurations of all IP address groups are displayed.

Configuration Example

1. Display the configurations of an IP address group.

```
FS#show ip-group 1

ip-group 1
```

```
description test
 ip-range 1.1.1.2 1.1.1.10
 ip-subnet 10.10.10.0 24
 ip-range 10.10.10.10 10.10.10.15
 ip-subnet 10.10.11.0 30
 ip-range 20.10.10.10 20.10.20.200
```

17.7 show ip-group statistics

Display IP address group statistics.

show ip-group statistics

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged mode, global configuration mode, or interface configuration mode

Default Level 14

Usage Guide If the **id** parameter is set, the routing information of the corresponding IP address group is displayed. If the **id** parameter is not set, the routing information of all IP address groups is displayed.

Configuration Example Display IP address group statistics.

```
FS#show ip-group statistics
ip-group server: 1.1.1.1
ip-group state: down
ip-group cnt: 0.
ip-group add event: 0.
ip-group del event: 0.
ip-group syn event: 0.
ip-group error event: 0.
ip-group enq err event: 0.
ip-group add table failed: 0
ip-group del table failed: 0
ip-group add entry failed: 0
ip-group del entry failed: 0
ip-group db-acct cnt: 0
```

Field description:

Field	Description
ip-group server	IP address of the server to which the database is connected
ip-group state	Database connection status
ip-group add event	Statistics on added IP addresses
ip-group del event	Statistics on deleted IP addresses
ip-group syn event	Statistics on synchronized IP addresses
ip-group error event	Statistics on incorrect IP addresses received
ip-group enq err event	Statistics on IP address enqueue errors
Ip-group add table failed	Number of failures in adding routing tables
Ip-group del table failed	Number of failures in deleting routing tables
Ip-group add entry failed	Number of failures in adding entries
Ip-group del entry failed	Number of failures in deleting entries
ip-group db-acct cnt	Acct table synchronization times

18 Link SAM Commands

18.1 clear link-sam statistics

Clear statistics on Link SAM with SAM+ system integration.

clear link-sam statistics [ace]

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged mode, global configuration mode, or interface configuration mode

Default Level 14

Usage Guide Run this command to clear statistics on Link SAM with SAM+ system integration.

Configuration Example

1. Clear statistics on Link SAM with SAM+ system integration.

```
FS# clear link-sam statistics
```

2. Clear statistics on traffic accounting.

```
FS# clear link-sam statistics ace
```

18.2 link-sam auth-server ip

Specify the authentication and accounting server.

link-sam auth-server ip *ip-address* **[port** *port-number***]**

Delete the authentication and accounting server.

no link-sam auth-server ip *ip-address*

Parameter Description

Parameter	Description
ip-address	IP address of the SAM+ authentication and accounting server.
port-number	Port number of the SAM+ authentication and accounting server. The default value is 4739.

Defaults By default, the SAM+ authentication and accounting server is not specified.

Command Mode Global configuration mode

Default Level 14

Usage Guide

Run this command to enable the ACE (client) to send traffic usage statistics to the SAM+.

Configuration Example

1. Specify the SAM+ authentication and accounting server.

```
FS(config)#link-sam auth-server ip 192.168.1.100
```

2. Delete the SAM+ authentication and accounting server.

```
FS(config)# no link-sam auth-server ip 192.168.1.100
```

Verification

Run the **show link-sam statistics ace** command to display statistics on traffic accounting.

18.3 link-sam conn-timeout

Set the Link SAM with SAM+ system integration timeout time.

link-sam conn-timeout *minutes* **[ace]**

Restore the default timeout time.

no link-sam conn-timeout [ace]

Restore default settings.

default link-sam conn-timeout [ace]

Parameter Description

Parameter	Description
minutes	Indicates the Link SAM with SAM+ system integration timeout time. The value ranges from 2 to 150,000, in minutes.

Defaults

The default timeout time is 2 minutes for traffic accounting and 20 minutes for non-traffic accounting.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use the default timeout time unless otherwise specified.

Configuration Example

1. Set the Link SAM with SAM+ system integration timeout time to 5 minutes.

```
FS(config)#link-sam conn-timeout 5
```

2. Restore the default timeout time.

```
FS(config)#nolink-sam conn-timeout
```

Verification

Run the **show link-sam statistics** command to display statistics on Link SAM with SAM+ system integration.

18.4 link-sam enable

Enable the Link SAM module.

link-sam enable

Disable the Link SAM module.

no link-sam enable

Restore default settings.

default link-sam enable

Parameter Description

Parameter	Description
address	IP address of the remote database

Defaults

By default, the Link SAM module is disabled.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Run this command to enable the ACE to send online user information to the SAM+ through the Link SAM module.

Configuration Example

1. Enable the Link SAM module.

```
FS(config)#link-sam enable
```

2. Disable the Link SAM module.

```
FS(config)#no link-sam enable
```

3. Connect the Link SAM module to a database.

```
FS(config)#link-sam enable db-ip 192.168.1.1
```

Verification

Run the **show link-sam statistics** command to display statistics on Link SAM with SAM+ system integration.

18.5 link-sam flowrate

Configure Link SAM rate limiting.

link-sam flowrate *rate*

Restore the default Link SAM rate, which is 22 packets per second.

no link-sam flowrate

Restore default settings.

default link-sam flowrate

Parameter Description

Parameter	**Description**
rate	Rate at which the Link SAM module is controlled to send packets, in the range from 1 to 65,535

Defaults

The default Link SAM rate is 22 packets per second.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use the default rate unless otherwise specified.

Configuration Example

1. Set the Link SAM rate to 50.

```
FS(config)#link-sam flowrate 50
```

2. Restore the default Link SAM rate.

```
FS(config)#nolink-sam flowrate
```

Verification

Run the **show link-sam statistics ace** command to display statistics on traffic accounting.

18.6 link-sam port

Configure the local listening port for the Link SAM module.

link-sam port *port* **[ace]**

Restore the default port number.

no link-sam port *port* **[ace]**

Restore default settings.

default link-sam port *port* **[ace]**

Parameter Description

Parameter	**Description**
port	TCP port number, in the range from 1 to 65535

Defaults

The default listening port is Port 2009 for traffic accounting and Port 2012 for non-traffic accounting.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use the default port unless otherwise specified.

Configuration Example

1. Configure Port 20000 as the local listening port for the Link SAM module.

```
FS(config)#link-sam port 20000
```

2. Restore the default port number.

```
FS(config)#no link-sam port
```

Verification

Run the **show link-sam statistics** command to display statistics on Link SAM with SAM+ system integration.

18.7 link-sam protocol

Configure the protocol version of the Link SAM module.

link-sam protocol { **v1** | **v2** }

Restore the default protocol version.

no link-sam protocol

Restore default settings.

default link-sam protocol

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the v2 protocol version is used.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

When configuring Link SAM with SAM+ system integration, check the protocol version of the Link SAM module to avoid communication failure due to version inconsistency. If you do not know the protocol version of the Link SAM module, run the **show link-sam statistics** command to check whether the value of the **exception messages** field increases greatly. If the value does not change, protocol versions may be inconsistent.

Configuration Example

1. Set the protocol version of the Link SAM module to v2.

```
FS(config)#link-sam protocol v2
```

2. Restore the default protocol version.

```
FS(config)#no link-sam protocol
```

Verification

Run the **show link-sam statistics** command to display statistics on Link SAM with SAM+ system integration.

18.8 show link-sam statistics

Display statistics on Link SAM with SAM+ system integration.

show link-sam statistics [ace]

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

Run this command to display the statistics of the SAM+ correlated with the Link SAM module.

Configuration Example

1. Display statistics on traffic accounting.

```
FS# show link-sam statistics ace

>Link-sam run state: enable

>Link-sam connect port: 2009

>Link-sam connect timeout minutes: 2

>Current SAM connections: 2

>Count of SAM connections: 2

>Count of SAM disconnections: 0

-----------------------------------------------------------------

link-sam flowrate 50

link-sam auth-server ip 192.168.1.100

link-sam auth-server ip 192.168.1.109 port 8000

-----------------------------------------------------------------
```

```
SAM's ip: 192.168.1.1

    Received packets: 2650

    Received user online messages: 530

    Received user offline messages: 0

    Received user synchronization messages: 2120

    Received user ip update messages: 0

    Received exception messages: 0

    Received invalid segments: 0


SAM's ip:192.168.10.1

    Received packets: 2400

    Received user online messages: 480

    Received user offline messages: 0

    Received user synchronization messages: 1920

    Received user ip update messages: 0

    Received exception messages: 0

Received invalid segments: 0
```

2. Display statistics on Link SAM with SAM+ system integration.

```
FS# show link-sam statistics

>Link-sam run state: enable

>Link-sam connect port: 2012

>Link-sam connect timeout minutes: 20

>Current SAM connections: 2

>Count of SAM connections: 2

>Count of SAM disconnections: 0

-------------------------------------------------------------------

SAM's ip: 192.168.1.1

    Received packets: 2650

    Received user online messages: 530

    Received user offline messages: 0

    Received user synchronization messages: 2120

    Received user ip update messages: 0

    Received exception messages: 0

    Received invalid segments: 0
```

```
SAM's ip:192.168.10.1
    Received packets: 2400
    Received user online messages: 480
    Received user offline messages: 0
    Received user synchronization messages: 1920
    Received user ip update messages: 0
    Received exception messages: 0
Received invalid segments: 0
```

Field description:

Field	Description
state	Status of Link SAM with SAM+ system integration
port	TCP port
timeout	Link SAM with SAM+ system integration timeout time
connections	Number of connections to the SAM+ server
disconnections	Number of disconnections from the SAM+ server
flowrate	Limited rate
auth-server	Information of the SAM+ authentication and accounting server
ip	IP address of the SAM+ authentication and accounting server
packets	Number of packets related to Link SAM with SAM+ system integration
messages	Number of messages related to Link SAM with SAM+ system integration
segments	Number of invalid records on Link SAM with SAM+ system integration

3. 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.
```

Field description:

Field	Description
run state	Whether Link SAM DB is enabled
server	IP address of the database
state	Status of Link SAM DB
cnt	Database reconnection times
syn event	Number of database synchronization requests of the accounting module
fail event	Number of traffic update failures
Online event	Number of database online notification events
Offline event	Number of database offline notification events
Error event	Number of database packet error notification events

19 Flow Account Commands

19.1 ipfix direct-url

Configure URL records for the IPFIX module.

ipfix direct-url *url*

Delete URL records from the IPFIX module.

no ipfix direct-url *url*

Parameter Description

Parameter	Description
url	URL records

Defaults

By default, no URL records are configured.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

To exempt some URLs from accounting, configure corresponding URL records for the IPFIX module (up to 1,000 URLs can be added).

Configuration Example

1. Configure a URL record for the IPFIX module.

```
FS(config)# ipfix direct-url www.baidu.com
```

2. Delete a URL record from the IPFIX module.

```
FS(config)#no ipfix direct-url www.baidu.com
```

Verification

Run the **show ipfix direct-url** command to display the URL resolution records of the IPFIX module.

19.2 ipfix enable

Enable the IPFIX module.

ipfix enable

Disable the IPFIX module.

no ipfix enable

Restore default settings.

default ipfix enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, the IPFIX module is disabled.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Enable the IPFIX module if IPFIX must be supported.

Configuration Example

1. Enable the IPFIX module.

```
FS(config)# ipfix enable
```

2. Disable the IPFIX module.

```
FS(config)#no ipfix enable
```

Verification

Run the **show ipfix configure** command to check whether the IPFIX module is enabled.

19.3 ipfix policy

Configure IPFIX policies.

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* **]**

Ipfix policy *num* **disable**

Delete IPFIX policies.

no ipfix policy *num*

Restore the effectiveness of IPFIX policies.

no ipfix policy *num* **disable**

Restore default settings.

default ipfixpolicy *num*

default ipfixpolicy *num* **disable**

Parameter Description

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.

home | foreign | campus | unicom | telecom | cmcc | cernet | cernet2 | direct-flow	Indicates the matched traffic type. Options: **home**: domestic traffic **foreign**: international traffic **campus**: campus traffic **unicom**: China Unicom **telecom**: China Telecom **cmcc**: China Mobile **cernet**: China Education and Research Network **cernet2**: second-generation China Education and Research Network **direct-flow**: traffic exempt from accounting
id	Indicates the interface ID (the interface must be a non-LAN interface).

Defaults

The default IPFIX policy is campus traffic matching.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Only the **home**, **foreign**, and **campus** options can be selected in SAM mode. In DB mode, all options can be selected.

When **group-id** is set to **0** for src-group and dst-group, any traffic types are matched.

Configuration Example

1. Configure an IPFIX policy to match domestic traffic.

```
FS(config)# ipfix policy 1 acl 1 action home interface GigabitEthernet 0/5
```

2. Disable an IPFIX policy.

```
FS(config)# ipfix policy 1 disable
```

Verification

Run the **show ipfix configure** command to display the IPFIX module configurations.

Common Errors

ACL binding is configured but ACLs are not configured.

19.4 ipfix policy change-pri

Adjust the priorities of IPFIX policies.

ipfix policy change-pri *num1 num2*

Parameter Description

Parameter	Description
num1	Indicates the name of Policy 1. The value ranges from 1 to 100.

num2	Indicates the name of Policy 2. The value ranges from 1 to 100.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Configuration Example Adjust the priorities of IPFIX policies.

```
FS(config)#ipfixpolicy change-pri 1 2
```

Verification Run the **show ipfix policy** command to display IPFIX policy priorities.

19.5 ipfix refresh enable

Enable IPFIX no-traffic detection.

Ipfix refresh enable

Disable IPFIX no-traffic detection.

no ipfix refresh enable

Restore default settings.

default ipfix refresh enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, IPFIX no-traffic detection is disabled.

Command Mode Global configuration mode

Default Level 14

Usage Guide Enable IPFIX no-traffic detection when necessary.

Configuration Example 1. Enable IPFIX no-traffic detection.

```
FS(config)# ipfix refresh enable
```

2. Disable IPFIX no-traffic detection.

```
FS(config)#no ipfix refresh enable
```

Verification Run the **show ipfix configure** command to check whether IPFIX no-traffic detection is enabled.

19.6 ipfix refresh-time

Set the IPFIX no-traffic detection period.

Ipfix refresh-time *time*

Restore the default detection period.

no ipfix refresh-time

Restore default settings.

default ipfix refresh-time

Parameter Description

Parameter	**Description**
time	Indicates the no-traffic detection period. The value ranges from 600 to 3,600, in seconds.

Defaults The default IPFIX no-traffic detection period is 600s.

Command Mode Global configuration mode

Default Level 14

Usage Guide Set the IPFIX no-traffic detection period to enable the IPFIX module to periodically detect users' traffic usage. If traffic usage is zero, the IPFIX module sends an abnormal go-offline message to the SAM.

Configuration Example Set the IPFIX no-traffic detection period.

```
FS(config)#ipfixrefresh-time1200
```

Verification Run the **show ipfix configure** command to display the IPFIX module configurations.

19.7 ipfix threshold enable

Configure IPFIX traffic threshold notification.

Ipfix threshold enable

Disable IPFIX traffic threshold notification.

no ipfix threshold enable

Restore default settings.

default ipfix threshold enable

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults By default, IPFIX traffic threshold notification is disabled.

Command Mode Global configuration mode

Default Level 14

Usage Guide Configure traffic threshold notification to enable the IPFIX module to notify the SAM when traffic usage is smaller than the threshold.

Configuration Example

1. Enable IPFIX traffic threshold notification.

```
FS(config)#ipfix threshold enable
```

2. Disable IPFIX traffic threshold notification.

```
FS(config)#no ipfix threshold enable
```

Verification Run the **show ipfix configure** command to display the IPFIX module configurations.

19.8 show ipfix direct-url

Display IPFIX URL records.

show ipfix direct-url

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged mode, global configuration mode, or interface configuration mode

Default Level 14

Usage Guide To display IPFIX URL records, run the **show ipfix direct-url** command.

Configuration Example

1. Display IPFIX URL records.

```
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
```

Field description:

Field	Description
URL	URL record
RESOLVE-IP	Resolved IP address

19.9 show ipfix configure

Display the IPFIX module configurations.

show ipfix configure

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

To display the IPFIX module configurations, run the **show ipfix configure** command.

Configuration Example

Display the IPFIX module configurations.

```
FS#show ipfix configure

ipfix configure:

ipfix state: enable

ipfix threshold state: enable

ipfix refresh-time: 900

ipfix policy 1 acl 1 action home

ipfix policy 2 acl 2 action foreign interface GigabitEthernet 0/3

ipfix policy 3 acl 3 action campus interface GigabitEthernet 0/5

ipfix policy 3 disable
```

Field description:

Field	Description
state	Indicates whether the IPFIX module is enabled.
threshold state	Indicates whether IPFIX traffic threshold notification is

	enabled.
refresh-time	Indicates the no-traffic detection period.
policy	Indicates IPFIX policies.

19.10 show ipfix online

Display online user information.

show ipfix online [user *user-name* **| ip** *ip-addr*| **count]**

Parameter Description

Parameter	Description
user-name	User ID
ip-addr	User's IP address

Command Mode

Privileged mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

To display online user information, run the **show ipfix online [user** *user-name* **| ip** *ip-addr*| **count]** command.

Configuration Example

1. Display all IPFIX egress statistics.

```
FS# show ipfixonline

User-id Ip    Sam-time     Sam-flow     Time          Flow          Campus          Home      Foreign

---------- ---------- ---------- ---------- ---------- ------------ ------ -----------------

11.1.1.1 36001024600            512              128/128         128/128         0/0

22.2.2.2    3600      1024           600            512      128/128         128/1238        0/0
```

2. Display the IPFIX egress statistics by user ID.

```
FS# show ipfixonline user 1

User-id Ip    Sam-time     Sam-flow     Time          Flow          Campus          Home      Foreign

---------- ---------- ---------- ---------- ---------- ------------ ------ -----------------

11.1.1.1 36001024600            512              128/128         128/128         0/0
```

3. Display the IPFIX egress statistics by IP address.

```
FS# show ipfixonline ip 1.1.1.1

User-id Ip    Sam-time     Sam-flow     Time          Flow          Campus          Home      Foreign

---------- ---------- ---------- ---------- ---------- ------------ ------ -----------------

11.1.1.1 36001024600            512              128/128         128/128         0/0
```

4. Display online user statistics.

```
FS# show ipfix online count

Online: 0

Max-online: 1
```

Field description:

Field	Description
User-id	User ID
Ip	User's IP address
Sam-time	Available extranet access duration that the SAM+ is notified of
Sam-flow	Available traffic that the SAM+ is notified of
Time	Time elapsed
Flow	Traffic used
Campus	Uplink and downlink campus traffic of users
Home	Uplink and downlink domestic traffic
Foreign	Uplink and downlink international traffic

19.11 show ipfix policy

Display the IPFIX policy status.

show ipfix policy

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged mode, global configuration mode, or interface configuration mode

Default Level

14

Usage Guide

To display the IPFIX policy status, run the **show ipfix policy** command.

Configuration Example

1. Display the IPFIX policy status.

```
FS# show ipfixpolicy

Policy      Acl         Src-grp     Dst-grp     Priority    Interface   Action      Disable     State

----------  ----------  ----------  ----------  ----------  ----------  ---------- ---------- ----------

1           1           0           0           0           Global      home        n
active

2           1           1           00          Gi0/5       foreign     n           active
```

Field description:

Field	Description
Policy	Policy name
Acl	ACL ID
Src-grp	Source ip-group
Dst-grp	Destination ip-group
Priority	Policy priority
Interface	Interface ID
Action	Matched traffic type
Disable	Whether the policy is enabled
State	Policy status

20 APP-AUTH Commands

20.1 app-auth ad-url

Use this command to set a URL to be redirected to during application authentication.

app-auth ad-url *string*

Use the **no** form of this command to delete the URL.

no app-auth ad-url

Parameter Description

Parameter	Description
string	Specifies a URL to be redirected to.

Defaults

No URL to be redirected to is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1. During embedded authentication, the URL to be redirected to is usually used to push an advertisement.
2. During authentication by associating with the server, the URL is usually set to an external portal address.

Configuration Example

#Configure the URL of the FS official website as the URL to be redirected to.

```
FS(config)# app-auth ad-url http://www.FS.com.cn
```

Verification

Run the **show app-auth statistics command** to display the URL to be redirected to.

```
FS#show app-auth statistics
------------------------------start---------------------------------
app_auth_enable: on
cwmp_enable: on
cwmp_bak: on
non_http_pass: off
device_serialno: 1234942570024
basename: 401034053077
portal_key: FS
g_wan_ip: 172.18.124.109
priv_info:
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:http://www.FS.com.cn
avoid app_name:
            directApp(247-250-0-0)
auth app_name:
            authModeApp(247-251-0-0)
auth_url:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 8878, rcv_query_msg_num: 0
----------------------------------end--------------------------------
```

20.2 app-auth auth-rule

Use this command to set a network segment for application authentication.

app-auth auth-rule ip *start-ip* **[** *end-ip* **]**

Use the **no** form of this command to delete the network segment.

no app-auth auth-rule ip *start-ip* [*end-ip*]

Parameter Description

Parameter	Description
start-ip	Specifies a start IPv4 address.
end-ip	Specifies an end IPv4 address.

Defaults No network segment is configured by default. After APP-AUTH is enabled, all users must be authenticated.

Command Mode Global configuration mode

Default Level 14

Usage Guide If no network segment is configured, all users will be authenticated through APP-AUTH. After a network segment is configured, only users within the network segment will be authenticated through APP-AUTH.

Configuration Example #Configure 192.168.1.0/24 as a network segment for application authentication.

```
FS(config)# app-auth auth-rule ip 192.168.1.1 192.168.1.255
```

Verification Run the **show app-auth auth-rule ip** command to display the network segment to be authenticated.

```
FS#show app-auth auth-rule
auth rule ip:
            192.168.1.1 - 192.168.1.255
```

20.3 app-auth cfg-opt

Use this command to configure application authentication options.

app-auth cfg-opt [**id-ip** | **id-mac** | **rdt-for-wx2** | **rdt-fo-wifidog** | **tup** *num* | **local-relay** [**enable** | **port** *port-num* | **exclude-online** | **syn-proxy** {**count** *syn-num*}]

Parameter Description

Parameter	Description
id-ip	Indicates a L3 network, and uses IP addresses to identify users.
id-mac	Indicates a L2 network, and uses MAC addresses to identify users.
rdt-for-wx2	Specifies the URL format of WiFi connection over WeChat 3.X.
rdt-for-wifidog	Specifies the URL format of WiFiDog authentication.
tup	Specifies the temporary allowed access function for the iOS system, which is used to control the iOS pop-up window.
num	Specifies the temporary allowed access time in seconds for the iOS system.
local-relay	Specifies the local relay function for URL redirection.
enable	Enables the relay function.
port	Specifies the relay port for redirection. This port must be consistent with that of the Webservice process.
port-num	Specifies the listening port for the Webservice process.
exclude-online	Excludes online users from traffic monitoring.
syn-proxy	Enables the SYN packet monitoring proxy.
syn-num	Specifies the number of SYN packet retransmission times before a proxy is enabled.

Defaults

1. On a L2 network, users are identified based on MAC addresses only by default.
2. Application identification dependency is enabled by default.
3. TR-069 is used for redirection by default.
4. The allowed iOS pass-through time is 120 seconds by default.
5. The local relay function is enabled by default.
6. Port 2060 is used as the relay port by default.
7. Traffic monitoring is performed online users by default.
8. Monitoring via a proxy is enabled on SYN packets by default, and the proxy is enabled if the number of SYN packet retransmission times reaches 3.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

1. IP addresses may be used to identify users on a L3 network, and MAC addresses are used to identify users on a L2 network.
2. Application identification dependency must be enabled during configuration of authentication applications and authentication-free applications.
3. If an external server is used for web authentication, parameters will be added behind the advertisement URL according to the URL format of the external server.

Configuration

#Identify a user based on an IP address.

Example

```
FS(config)#app-auth cfg-opt id-ip
```

#Choose the URL format of WiFiDog authentication.

```
FS(config)#app-auth cfg-opt rdt-for-wifidog
```

Verification

Run the **show app-auth cfg-opt** command to display the enabled authentication options.

```
FS#show app-auth cfg-opt
pp_auth_cfg_id: 1
app_auth_cfg_rdt_style: 8
app_auth_rdt_style_str: app-auth
app_auth_cfg_rdt_mode_url: 0
app_auth_cfg_strict_tup: 1
app_auth_cfg_dep_idy: 1
app_auth_cfg_aply_ref: 0
app_auth_cfg_proxy:1
app_auth_cfg_relay_enable: 1
app_auth_cfg_relay_port: 2060
app_auth_cfg_relay_enhance: 1
app_auth_enable_mac_inq: 1
app_auth_cfg_strict_tup: 1
app_auth_cfg_no_detect_online: 0
app_auth_cfg_rdt_style_302: 1
```

If the value of app_auth_cfg_id is 1, a L2 network is used, and users are identified based on MAC addresses. If the value is 2, a L3 network is used, and users are identified based on IP addresses.

Platform Description

This command is supported only on gateway series products.

20.4 app-auth clear

Use this command to clear all denied MAC addresses.

app-auth clear deny-mac

Use this command to clear all allowed MAC addresses.

app-auth clear direct-mac

Use this command to clear all authentication-free URLs of extranets.

app-auth clear direct-url

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Command Mode

Privileged EXEC mode

Default Level 14

Usage Guide Use the clear commands to clear preceding configurations before an external server delivers a command, to avoid impact of the preceding configurations.

Configuration Example

Verification

20.5 app-auth cwmp enable

Use this command to enable the external authentication function.

app-auth cwmp enable

Use the **no** form of this command to disable the external authentication function.

no app-auth cwmp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The external authentication function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide After the external authentication function is enabled, an external server controls go-online behaviors of users. A gateway sends an attention message to the server in order to match an application or a URL, and the server determines, based on settings, whether to pass the authentication of a user.

Configuration Example #Enable the external authentication function.

```
FS(config)# app-auth cwmp enable
```

Verification Run the **show app-auth statistics** command to display the switch status of APP-AUTH.

```
FS#show app-auth statistics
------------------------------start---------------------------------
app_auth_enable: off
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:
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:
auth app_name:
auth_url:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
---------------------------------end-------------------------------
```

If the value of **cwmp_enable** is **off**, the external authentication function is disabled. If the value is **on**, the external authentication function is enabled.

20.6 app-auth deny-mac

Use this command to deny intranet MAC addresses.

app-auth deny-mac *mac_addr* [**aging-time** *time*] [**comment** *string*]

Use the **no** form of this command to delete authentication-free extranet IP addresses.

no app-auth deny-mac *mac_addr*

Parameter Description

Parameter	Description
mac_addr	Specifies an intranet MAC address.
time	Specifies aging time in the unit of minute.
string	Describes this configuration.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to deny intranet MAC addresses from Internet access. This command is used for L2 networks.

Configuration Example

#Deny the MAC address 00d0.11ff.2233 from Internet access.

```
FS(config)# app-auth deny-mac 00d0.11ff.2233
```

Verification

Run the **show app-auth deny-mac** command to display the configuration result.

```
app-auth deny-mac num: 1
            mac: 00d0.11ff.2233, flag: 1
```

Platform Description

This command is supported only on gateway series products.

20.7 app-auth direct-app

Use this command to configure authentication-free applications.

app-auth direct-app *app-name*

Use the **no** form of this command to delete authentication-free applications.

no app-auth direct-app *app-name*

Parameter Description

Parameter	Description
app-name	Specifies an application name.

Defaults

-

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to configure an identified application as an authentication-free application and allow access requests to the application.

Configuration Example

#Allow all access requests to a microblog application.

```
FS (config)# app-auth direct-app Sina Microblog
```

Verification

1. Run the **show app-auth statistics** command to display the configuration result of the application.

```
FS(config)#show app-auth statistics
------------------------------start---------------------------------
app_auth_enable: off
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:
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:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
----------------------------------end--------------------------------
```

The **avoid app_name** field corresponds to authentication-free applications.

2. Attempt to access the application and check whether the application can be directly accessed without authentication.

20.8 app-auth direct-dstip

Use this command to configure authentication-free extranet IP addresses. If an end IP address is not configured, a single IP address is configured by default.

app-auth direct-dstip *ip_start* **[** *ip_end* **] [aging-time** *time* **] [comment** *string* **]**

Use the **no** form of this command to delete authentication-free extranet IP addresses.

no app-auth direct-dstip *ip_start* **[** *ip_end* **]**

Parameter Description

Parameter	Description
ip_start	Specifies a start IPv4 address.
ip_end	Specifies an end IPv4 address.
time	Specifies aging time in the unit of minute.
string	Describes this configuration.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide

Use this command to add the IP address of a server into the authentication-free extranet IP address list to allow direct access to the server without authentication.

Configuration Example

#Configure 3.3.3.3 as an authentication-free extranet IP address.

```
FS(config)# app-auth direct-dstip 3.3.3.3
```

Verification

1. Run the **show app-auth direct-dstip** command to display the authentication-free extranet IP address.

```
FS(config)#show app-auth direct-dstip
direct dst-ip:
          3.3.3.3
```

2. Enable APP-AUTH, attempt to directly access the extranet IP address without authentication, and check whether the access is successful.

Platform Description

This command is supported only on gateway series products.

20.9 app-auth direct-mac

Use this command to configure authentication-free intranet MAC addresses.

app-auth direct-mac *mac_addr* [**aging-time** *time*] [**comment** *string*]

Use the **no** form of this command to delete authentication-free intranet MAC addresses.

no app-auth direct-mac *mac_addr*

Parameter Description

Parameter	Description
mac_addr	Specifies an intranet MAC address.
time	Specifies aging time in the unit of minute.
string	Describes this configuration.

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to configure authentication-free intranet MAC addresses. This command is used for L2 networks.

Configuration Example

#Configure 00d0.11ff.2233 as an authentication-free MAC address.

```
FS(config)# app-auth direct-mac 00d0.11ff.2233
```

Verification

Run the **show app-auth direct-mac** command to display the configuration result.

```
app-auth direct-mac num: 1
          mac: 0010.1144.3344, flag: 0
```

20.10 app-auth direct-srcip

Use this command to configure authentication-free intranet IP addresses. If an end IP address is not configured, a single IP address is configured by default.

app-auth direct-srcip *ip_start* **[** *ip_end* **] [aging-time** *time* **] [comment** *string* **]**

Use the **no** form of this command to delete authentication-free intranet IP addresses.

no app-auth direct-srcip *ip_start* **[** *ip_end* **]**

Parameter Description

Parameter	**Description**
ip_start	Specifies a start IPv4 address.
ip_end	Specifies an end IPv4 address.
time	Specifies aging time in the unit of minute.
string	Describes this configuration.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to add the IP address of a PC into the authentication-free intranet IP address list to allow the PC to directly access extranets without authentication.

Configuration Example #Configure 192.168.1.100–192.168.1.120 as an authentication-free network segment.

```
FS(config)# app-auth direct-srcip 192.168.1.100 192.168.1.120
```

Verification

1. Run the **show app-auth direct-srcip** command to display authentication-free intranet IP addresses.

```
FS(config)#show app-auth direct-srcip
direct src-ip:
            192.168.1.100 - 192.168.1.120
```

2. Enable APP-AUTH, attempt to directly access an extranet without authentication through the PC, and check whether the access is successful.

Platform Description This command is supported only on gateway series products.

20.11 app-auth direct-url

Use this command to configure authentication-free extranet URLs.

app-auth direct-url *string*

Use the **no** form of this command to delete authentication-free URLs.

no app-auth direct-domain *string*

Parameter

Parameter	**Description**

Description

string	Specifies a URL.

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to add URLs into an authentication-free URL list to allow direct access to the URLs without authentication.

This command supports URLs in https://, http://, and ftp:// formats. The gateway will not store these prefixes. If an HTTPS or FTP URL is configured, a client must initiate a DNS request before the gateway allows the client to access the URL.

Non-encrypted HTTP accesses are allowed. Accesses in other formats must be implemented based on client DNS learning.

Configuration Example

#Configure FS official website as an authentication-free URL.

```
FS(config)# app-auth direct-url http://www.FS.com.cn
```

Verification

1. Run the **show app-authd direct-url** command to display the authentication-free URL.

```
FS(config)#show app-auth direct-url
direct url:
        www.FS.com.cn
       ccbc.com.cn
```

The prefix http:// of URLs will be automatically deleted, and the prefixes https:// and ftp:// of other URLs will be reserved.

2. Enable APP-AUTH, attempt to directly access the URL without authentication through a PC, and check whether the access is successful.

20.12 app-auth enable

Use this command to enable APP-AUTH.

app-auth enable

Use the **no** form of this command to disable APP-AUTH.

no app-auth enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

APP-AUTH is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Users cannot access the Internet without authentication after APP-AUTH is enabled.

Configuration Example

#Enable APP-AUTH.

```
FS(config)# app-auth enable
```

Verification

Run the **show app-auth statistics** command to display the switch status of APP-AUTH.

```
FS#show app-auth statistics
------------------------------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:
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:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
----------------------------------end--------------------------------
```

Platform Description

This command is supported only on gateway series products.

20.13 app-auth kick

Use this command to kick off an online node that has passed the application authentication.

app-auth kick ip *ip-addr*

Use this command to kick off all online nodes.

app-auth kick all

Parameter Description

Parameter	Description
ip-addr	Specifies an IPv4 address.

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide Search for online nodes according to IP addresses, and kick them off for re-authentication.

After APP-AUTH is disabled, all online nodes must be kicked off.

Configuration Example #Kick the online client with the IP address 2.2.2.2 off.

```
FS# app-auth kick-ip 2.2.2.2
```

Verification Before kicking the client off, run the **show app-auth online** command to display the online nodes.

After kicking the client off, run the **show app-auth online** command to check whether the client is online.

20.14 app-auth local-auth authorize

Use this command to configure the QR code authorization function.

app-auth local-auth authorize { **check** | **restrict-times** *times* }

Use this command to set the default number of times that an authorized user can grant the Internet access permission to other users.

no app-auth local-auth authorize restrict-times *times*

Use the **no** form of this command to disable the QR code authorization function.

no app-auth local-auth authorize check

Parameter Description

Parameter	Description
times	Specifies the number of authorization times.

Defaults The function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Example #Enable QR code authorization-based authentication on the gateway and set 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
```

Verification Run the **show app-auth local-auth config** command to display the 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        state:    Not exist
  pc:
    global: false
    name:
    state:    Idle
```

Platform Description This command is supported on gateway series products.

20.15 app-auth local-auth authorize-time

Use this command to set the available online duration of an authorized user.

app-auth local-auth authorize authorize-time *minute*

Use the **no** form of this command to restore the default available online duration.

no app-auth local-auth authorize-time

Parameter Description

Parameter	Description
minute	Specifies the available online duration after authorized authentication.

Defaults

This command is not configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Enable QR authorization-based authentication on the gateway and set the available online duration to 60 minutes for authenticated users.

```
FS# configure terminal
FS(config)# app-auth local-auth authorize-time 60
```

Verification

Run the **show app-auth local-auth config** command to display the 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        state:    Not exist
```

```
pc:
    global: false
    name:
    state:    Idle
```

Platform Description This command is supported on gateway series products.

20.16 app-auth local-auth data-store

Use this command to configure the automatic aging time of information about locally authenticated users in the database.

app-auth local-auth data-store { **enable | age day** *day* }

Use this command to restore the default time.

no app-auth local-auth data-store age

Use the **no** form of this command to disable the automatic aging function.

no app-auth local-auth data-store enable

Parameter Description

Parameter	Description
day	Specifies the aging period.
enable	Enables the automatic aging function.

Defaults The function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Example #Set the 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

1. Run the **show app-auth local-auth config** command to display the configuration and check the value of **data-store-age-day**.

```
FS# show app-auth local-auth config
enable: True
data-store-enable: True
data-store-age-day: 5
```

```
user-mac-limit: 5
online-time: 1
authorize-time: 33
restrict-range information:
  mobile:
    global: true
    name:     day
    state:   Not exist
  pc:
    global: false
    name:
    state:   Idle
```

Platform Description

This command is supported on gateway series products.

20.17 app-auth local-auth enable

Use this command to enable local authentication.

app-auth local-auth enable

Use the **no** form of this command to disable local authentication.

no app-auth local-auth enable

Parameter Description

Parameter	Description
enable	Enables local authentication.

Defaults

Local authentication is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Enable local authentication.

```
FS(config)# app-auth local-auth enable
```

Verification

Run the **show app-auth local-auth config** command to display whether local authentication is enabled.

```
FS#show app-auth local-auth config
app-auth local-auth enable
```

Platform Description

This command is supported on gateway series products.

20.18 app-auth local-auth online-time

Use this command to configure the available online duration for local users who are successfully authenticated.

app-auth local-auth online-time *time*

Use the **no** form of this command to restore the default duration.

no app-auth local-auth online-time

Parameter Description

Parameter	Description
time	Specifies the duration, in minutes.

Defaults

The available online duration is not limited by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is unavailable to authorized users passing authentication.

Configuration Example

#Set the available online duration to 10 minutes for local users who are successfully authenticated on the gateway.

```
FS(config)# app-auth local-auth online-time 10
```

Verification

Run the **show app-auth local-auth config** command to display the 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
```

Platform Description

This command is supported on gateway series products.

20.19 app-auth local-auth restrict

Use this command to restrict clients in specific types from Internet access.

app-auth local-auth restrict { **pc** | **mobile** } [**exclude time-range** *time*]

Use the **no** form of this command to cancel client restriction from Internet access.

no app-auth local-auth restrict { **pc** | **mobile** }

Parameter Description

Parameter	Description
pc	Restricts PCs from Internet access.
mobile	Restricts mobile phones from Internet access.
time	Specifies the start time from which the Internet access is not restricted.

Defaults

The Internet access is not restricted by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to restrict the Internet access behaviors of users.

Configuration Example

#Restrict mobile users from Internet access except in the "day" time period.

```
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 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
```

Platform Description

This command is supported on gateway series products.

20.20 app-auth local-auth subscriber mac-limit

Use this command to configure the upper limit of clients that can be used by each locally authenticated user.

app-auth local-auth subscirber mac-limit *limit-num*

Use the **no** form of this command to restore the default settings.

no app-auth local-auth subscirber mac-limit

Parameter Description

Parameter	Description
limit-num	Specifies the limited quantity.

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Set the upper limit of clients that can be used by each locally authenticated user to 5.

```
FS# configure terminal
FS(config)# app-auth local-auth subscirber mac-limit 5
```

Verification

Run the **show app-auth local-auth config** command and check the value of **user-mac-limit**.

```
FS# show app-auth local-auth config
enable: True
data-store-enable: True
data-store-age-day: 36
```

```
user-mac-limit: 5
online-time: 1
authorize-time: 33
restrict-range information:
  mobile:
    global: true
    name:      day
    state:    Not exist
  pc:
    global: false
    name:
    state:    Idle
```

Platform Description

This command is supported on gateway series products.

20.21 app-auth local-auth subs-name

Use this command to configure information about a locally authenticated user.

app-auth local-auth subs-name *name* **type local**

Use the **no** form of this command to delete information about a locally authenticated user.

no app-auth local-auth subs-name *name* **type local**

Parameter Description

Parameter	Description
name	Indicates a username.
type	Indicates the user type.
local	Indicates a local user.

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Configure a user.

```
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 the configuration.

```
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
```

Platform Description

This command is supported on gateway series products.

20.22 app-auth local-auth vip-group

Use this command to configure a locally authenticated user as a VIP user.

app-auth local-auth vip-group *user-name* **local**

Use the **no** form of this command to delete a VIP user.

no app-auth local-auth vip-group *user-name* **local**

Parameter Description

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.

Defaults

N/A

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Configure a 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 information about the VIP user.

```
FS# FS# show app-auth local-auth vip-group all

cnt: 1/100. ad_any_vip: 0
```

```
Group-name                                                              type          idx
------------------------------------------------------------------------------
aaa                                                                     local         0
```

Platform Description

This command is supported on gateway series products.

20.23 app-auth offline-detect

Use this command to configure the traffic-based client go-offline function.

app-auth offline-detect [time-interval *time* **flowrate** *flow***]**

Use the **no** form of this command to disable the function.

no app-auth offline-detect

Parameter Description

Parameter	**Description**
time	Specifies the monitoring time in the unit of minute. The value range is 1 to 65,535. The default value is 15.
flow	Specifies a bit rate in the unit of bps. The value range is 0 to 1,000,000. The default value is 0.

Defaults

The function is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Configure application authentication and force a client to go offline if the traffic rate of the client is lower than 10 kbps within 15 minutes.

```
FS(config)# app-auth offline-detect time-interval 15 flowrate 10000
```

Verification

After the traffic-based client go-offline function is configured and APP-AUTH is enabled, run the show **app-auth online** command to verify that a smartphone is offline if the shutdown time of the smartphone exceeds a specified interval.

Platform Description

This command is supported only on gateway series products.

20.24 app-auth portal-key

Use this command to set a key for data encryption.

app-auth portal-key *password*

Parameter Description

Parameter	Description
password	Configures a key to encrypt data during communication with a server.

Defaults No key is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Example #Configure a key as FS.

```
FS(config)# app-auth portal-key FS
```

Verification Run the **show app-auth statistics** command to display the configuration result.

20.25 app-auth priv-info

Use this command to configure private information of redirection.

app-auth priv-info *info*

Parameter Description

Parameter	Description
info	Specifies private information of redirection.

Defaults Private information of redirection is not configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to configure private information that can be carried during redirection.

Configuration Example #Set the site ID in redirection to **FS**.

```
FS(config)#app-auth priv-info siteid=FS
```

Verification Run the show **app-auth statistics** command to display the configuration result.

```
FS#show app-auth statistics
------------------------------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:
        Instant messaging (0-0-0-0)
auth_url:
        http://www.FS.com.cn

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
----------------------------------end--------------------------------
```

20.26 app-auth proxy-url

Use this command to set a URL of a proxy.

app-auth proxy-url *url* **{rdt-type** *num***}**

Use the **no** form of this command to delete the URL of a proxy.

no app-auth proxy-url

Parameter Description

Parameter	Description
url	Specifies the URL of a proxy. This parameter is set to an IP address as required, for example, http://10.1.0.6/redirect.
rdt-type	Configures a redirection method.
num	Specifies the number of a special redirection method.

Defaults No proxy URL is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to configure a special redirection method for the proxy URL if an authentication scheme is defined.

If the special redirection method is not numbered, the default redirection method is used.

The URL of the proxy cannot be distributed to an intranet server.

This command is used for WiFi connection over WeChat and custom application authentication modes.

Configuration Example #Set 10.1.0.6 as a URL of a proxy.

```
FS(config)#app-auth proxy-url http://10.1.0.6
```

Verification Run the **show app-auth statistics** command to display the configuration result.

```
FS#show app-auth statistics
------------------------------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:
        Instant messaging (0-0-0-0)
auth_url:
        http://www.FS.com.cn

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
----------------------------------end--------------------------------
```

Common Errors Private information of redirection is not configured by default. Negotiate with the customer about the private information to be carried according to specific projects.

Platform Description

This command is supported only on gateway series products.

20.27 app-auth policy

Use this command to add an authentication policy.

app-auth policy *name*

Use the **no** form of this command to delete an authentication policy.

no app-auth policy *name*

Parameter Description

Parameter	Description
name	Indicates a policy name.

Defaults

No authentication policy is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to add an authentication policy.

Configuration Example

#Configure an authentication policy named aaa.

```
FS(config)# app-auth policy aaa
```

Verification

Run the **show app-auth policy** command to display the configuration.

```
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
```

Platform Description This command is supported on gateway series products.

20.28 app-auth policy-swap

Use this command to swap the priorities of two policies.

app-auth policy-swap *rule-name1 rule-name2*

Parameter Description

Parameter	Description
rule-name1	Indicates the name of a policy whose priority needs to be swapped.
rule-name2	Indicates the name of a policy whose priority needs to be swapped.

Defaults This command is not configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to swap the priorities of two policies.

Configuration Example #Swap the priorities of rule1 and rule2.

```
FS(config)#app-auth policy-swap rule1 rule2
```

Verification Run the **show app-auth policy** command to display the configuration.

```
FS# show app-auth policy
app-auth policy rule2 type sms
app-auth policy rule1 type weixin
```

Platform Description This command is supported on gateway series products.

20.29 app-auth server

Use this command to configure an authentication server.

app-auth server *name* **type** { **act-directory** | **qrcode-alone** | **qrcode-authorize** | **sms** | **weixin** }

Use the **no** form of this command to restore the default settings.

no app-auth server *name*

Parameter Description

Parameter	Description
name	Indicates the server name.
act-directory	Indicates the AD domain server-based authentication.
qrcode-alone	Indicates authentication using self-help QR code scanning.
qrcode-authorize	Indicates authentication using authorized QR code scanning.
sms	Indicates SMS-based authentication.
weixin	Indicates WeChat-based authentication.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Example

#Configure an authentication server named abc 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 server all** command to display the configuration.

```
FS# show app-auth server all

server name: abc

type: qrcode-alone

     mode: alone

     comment: Welcome!

     ip: 2.2.2.2

     key: 1
```

Platform Description This command is supported on gateway series products.

20.30 app-auth set-ssid

Use this command to set an SSID.

app-auth set-ssid ssid {**ip-range** *ip-start ip-end}*

Parameter

Parameter	Description

Description

ssid	Specifies an SSID name.
ip-range	Configures an IPv4 address range.
ip-start	Specifies a start IPv4 address.
ip-end	Specifies an end IPv4 address.

Defaults No SSID is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide An SSID is used as a redirection parameter. If no network segment is configured, the SSID is valid globally. After a network segment is configured, only users within the network segment match the SSID.

Configuration Example #Set a global SSID to @@test.

```
FS(config)# app-auth set-ssid @@test
```

Verification Run the **show app-auth ssid-cfg** command to display the configuration result.

```
FS#show app-auth ssid-cfg
global: @@test
```

Platform Description This command is supported only on gateway series products.

20.31 app-auth snp enable

Use this command to enable DHCP snooping.

app-auth snp enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide In a L3 network environment, MAC addresses of clients can be obtained through DHCP snooping provided that DHCP snooping is enabled for the DHCP component. MAC addresses of clients must be obtained in WeChat authentication mode.

Configuration Example

#Enable DHCP snooping.

```
FS(config)#app-auth snp enable
```

Verification

Run the **show app-auth snp-cfg** command to display the configuration result.

```
FS#show app-auth snp-cfg
snp: 1
```

20.32 app-auth tcp-socket

Use this command to set a TCP keepalive connection.

app-auth tcp-socket [***enable*** | ***server*** *server-url* | ***keepalive*** *time_1* | ***user-inform*** *time_2*]

Parameter Description

Parameter	Description
enable	Enables the TCP keepalive connection function.
server	Configures a server.
server-url	Configures a server IP address.
keepalive	Specifies the TCP keepalive function.
time_1	Specifies a TCP keepalive period. The value range is 30 to 3,600 in seconds. The default value is 30.
user-inform	Synchronizes user information periodically.
time_2	Specifies a synchronization interval. The value range is 30 to 3,600 in seconds. The default value is 300.

Defaults

No TCP keepalive connection is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

After the function is enabled, the gateway can synchronize user information with servers. This function applies to authentication and accounting and other scenarios that impose a high requirement for user synchronization. If no server IP address is configured, the advertisement redirection URL is used by default.

Configuration Example

#Set the IP address for the TCP keepalive connection to 172.18.124.56.

```
FS(config)# app-auth tcp-socket server http://172.18.124.56
FS(config)# app-auth tcp-socket enable
```

Verification

Run the **show app-auth tcp** command to display the configuration result.

```
FS#show app-auth tcp-info
tcp_server_url: http://172.18.124.56
tcp_enable: 1
tcp_keepalive_period: 300
```

```
user_inform_period: 300
tcp_sock: -1
tcp_state: 1
server_ip: 0.0.0.0, port: 0
server_change: 1
rcv_pkt_num: 0
rcv_error_pkt_num: 0
keepalive_last_send_time: 0
keepalive_last_rcv_time: 0
user_inform_last_send_time: 0
user_inform_last_rcv_time: 0
```

20.33 app-auth tup-app

Use this command to configure temporarily authentication-free applications.

app-auth tup-app *app-name*

Use the **no** form of this command to delete temporarily authentication-free applications.

no app-auth tup-app *app-name*

Parameter Description

Parameter	Description
app-name	Specifies an application name.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to temporarily allow WeChat accesses if WeChat is triggered by a portal in WeChat connection over WiFi mode. The configuration is dependent on the portal.

Configuration Example #Temporarily allow WeChat accesses.

```
FS(config)# app-auth tup-app WeChat
```

Verification Run the **show app-auth statistics** command to display the configuration result of the application.

```
FS(config)#show app-auth statistics
------------------------------start---------------------------------
app_auth_enable: off
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:
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)
tup app_name:
        WeChat (7-10-0-0)
auth app_name:
auth_url:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
----------------------------------end--------------------------------
```

The **tup app_name** field corresponds to the temporarily allowed application.

Related Commands

Run the **show identify-application** command to display the application name in the application identification library.

Platform Description

This command is supported only on gateway series products.

20.34 app-auth set-hz

Use this command to set site IDs and site names.

app-auth set-hz siteid *id-num* **sitename** *name* { **ip-range** *ip-start ip-end* }

Parameter Description

Parameter	**Description**
id-num	Indicates a site ID.
name	Indicates a site name.
ip-start	Specifies a start IP address.
ip-end	Specifies an end IP address.

Defaults

No site ID or site name is configured by default.

Command Mode

Global configuration mode

Default Level 14

Usage Guide The site ID and site name are used as redirection parameters. If no network segment is configured, they are valid globally. After a network segment is configured, only users within the network segment match the site ID and site name.

Configuration Example #Set the global site ID to 111, and site name to FS.

```
FS(config)# app-auth set-hz siteid 111 sitename FS
```

Verification Run the **show app-auth hz-info** command to display the configuration result.

```
FS# show app-auth hz-info
{"root":{"siteid":"111", "sitename":"FS"}, "branch": [] }
```

20.35 app-auth proxy-option

Use this command to enable HTTPS redirection.

app-auth proxy-option [**https | session total** *total_limit* **per-ip** *per_ip_limit*]

Parameter Description

Parameter	Description
https	Indicates HTTPS redirection.
session total *total_limit*	Indicates the limit on the total number of sessions.
per-ip *per_ip_limit*	Indicates the limit on the number of sessions per IP address.

Defaults N/A

Command Mode Global configuration mode

Default Level 14

Usage Guide By running this command, all HTTPS traffic is redirected to s specified Portal page.

Configuration Example #Enable HTTPS redirection.

```
FS(config)# app-auth proxy-option https
```

#Configure the limit on the number of sessions.

```
FS(config)# app-auth proxy-option session total 10000 per-ip 200
```

Verification Run the **show app-auth proxy-option config** command to display the configuration.

```
FS#show app-auth proxy-option config
```

```
---------- App-Auth Option Config Info ----------
Redirect for https    : Enable
Session total limit : 20001
Session per-ip limit: 201
----------------------- End ---------------------
FS#
```

Platform Description

This command is supported on gateway series products.

20.36 local-auth qrcode

Use this command to configure QR code-based authentication.

local-auth qrcode { **ip** *ip-address* | **key** *key-str* | **comment** *comment-str* }

Use the **no** form of this command to delete the QR code-based authentication.

no local-auth qrcode { **ip** | **key** | **comment** }

Parameter Description

Parameter	Description
ip-address	Specifies the IP address for accessing the QR code.
key-str	Specifies the dynamic code of the QR code.
comment-str	Indicates the comment string.

Defaults

N/A

Command Mode

Authentication server mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Configure QR code-based authentication.

```
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
FS(config-app-auth-server)# local-auth qrcode key test
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
```

Platform Description This command is supported on gateway series products.

20.37 local-auth sms

Use this command to configure SMS-based authentication.

local-auth sms { **mode prior** | **server** { **aliyun-v1** | **aliyun-v2** } | **keyid** *id* **keysecret** *string* **sign** *string* **templet** string }

Use the **no** form of this command to delete the SMS-based authentication.

no local-auth sms { **mode prior** | **server** | **keyid** }

Parameter Description

Parameter	Description
keyid	Indicates the appkey for SMS server-based authentication.
keyid-str	Specifies the specific appkey.
keysecret	Indicates the secret-key for SMS-based authentication.
*keysecret-str***:**	Specifies the specific secret-key string.
sign	Indicates the SMS signature.
sign-str	Specifies the SMS signature string.
templet	Indicates the SMS template.
templet-str	Specifies the SMS template string.
server	Indicates the type of the SMS server.
aliyun-v1	Indicates Alibaba Cloud SMS v1.
aliyun-v2	Indicates Alibaba Cloud SMS v2.
mode	Indicates the SMS mode.
prior	Indicates the prior mode.

Defaults N/A

Command Mode Authentication server mode

Default Level 14

Usage Guide N/A

Configuration Example #Configure SMS-based authentication.

```
FS# configure terminal
FS(config)# app-auth server sms-auth type sms
FS(app-auth-policy)# local-auth sms keyid aaabbb keysecret cccddd sign eeefff templet ggghhh
FS(app-auth-policy)# local-auth sms server aliyun-v1
FS(app-auth-policy)# local-auth sms mode prior
```

Verification

Run the **show app-auth server all** command to display the 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
```

Platform Description

This command is supported on gateway series products.

20.38 local-auth weixin

Use this command to configure WeChat-based authentication.

local-auth weixin { **shopid** *shopid-str* **appid** *appid-str* **secretkey** *secretkey-str* | **ssid** *ssid-str* }

Use the **no** form of this command to delete the WeChat-based authentication.

no local-auth weixin { **shopid** | **ssid** }

Parameter Description

Parameter	Description
shopid-str	Indicates the shop ID.
appid-str	Indicates the app ID.
secretkey-str	Indicates the key.
ssid-str	Indicates the network SSID.

Defaults

N/A

Command Mode

Authentication server mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Configure WeChat-based authentication.

```
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
FS(config-app-auth-server)# local-auth weixin ssid ssid_test
```

Verification

Run the **show app-auth server all** command to display the 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
```

Platform Description

This command is supported on gateway series products.

20.39 mac

Use this command to configure client information of a locally authenticated user.

mac *mac-address* { **auto** | **manual** } **type** { **pc** | **mobile** }

Use the **no** form of this command to delete client information of a locally authenticated user.

no mac *mac-address*

Parameter Description

Parameter	**Description**
mac-address	Indicates the MAC address.
auto	Indicates that client information is automatically imported.
manual	Indicates that client information is manually configured.
pc	Indicates that the client is a PC.
mobile	Indicates that the client is a mobile device.

Defaults

N/A

Command Mode

APP-AUTH user configuration mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Configure a locally authenticated user and the user's client information.

```
FS# configure terminal
FS(config)# app-auth local-auth subs-name abc type ad
FS(config-app-auth-subs)# mac 0011.2233.4455 manual type pc
```

Verification

Run the **show app-auth local-auth subs all** command to display client information.

```
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
```

Platform Description

This command is supported on gateway series products.

20.40 relate server

Use this command to configure an authentication server associated with an authentication policy.

relate server *server-name*

Use the **no** form of this command to disable the authentication server associated with an authentication policy.

no relate server *server-name*

Parameter Description

Parameter	Description
server-name	Indicates the name of an authentication server.

Defaults

N/A

Command Mode

APP-AUTH policy configuration mode

Default Level

14

Usage Guide

This command can be configured only after a policy is configured.

Configuration Example

#Associate the WeChat authentication server with an authentication policy.

```
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 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
```

Platform Description

This command is supported on gateway series products.

20.41 rule enable

Use this command to enable a policy.

rule enable

Use the **no** form of this command to disable a policy.

no rule enable

Parameter Description

Parameter	Description
enable	Enables a policy.

Defaults

N/A

Command Mode

APP-AUTH policy configuration mode

Default Level 14

Usage Guide This command can be configured only after a policy is configured.

Configuration Example #Enable a rule.

```
FS(config)# app-auth policy aaa
FS(app-auth-policy)# rule enable
```

Verification Run the **show app-auth policy** command to display the 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
```

Platform Description This command is supported on gateway series products.

20.42 rule ip-range

Use this command to configure a network segment in which an authentication policy is effective.

rule ip-range { [*ip1* { *ip2* }] | **all** }

Use the **no** form of this command to delete the network segment.

no rule ip-range

Parameter Description

Parameter	**Description**
ip1	Indicates the start IP address of the network segment.
ip2	Indicates the end IP address of the network segment.
all	Indicates that the authentication policy takes effect on all IP addresses.

Defaults N/A

Command Mode APP-AUTH policy configuration mode

Default Level 14

Usage Guide The policy takes effect on IP addresses that are within the network segment.

Configuration Example

#Enable a policy to take effect on all IP addresses.

```
FS(config)# app-auth policy aaa
FS(app-auth-policy)# rule ip-range all
```

Verification

Run the **show app-auth policy** command to display the 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
```

Platform Description

This command is supported on gateway series products.

20.43 rule ssid

Use this command to configure the SSID for an authentication policy.

rule ssid *ssid*

Use the **no** form of this command to delete the SSID of an authentication policy.

no rule ssid

Parameter Description

Parameter	Description
ssid	Indicates the SSID of a policy.

Defaults

N/A

Command Mode

APP-AUTH policy configuration mode

Default Level

14

Usage Guide

N/A

Configuration Example

#Configure an authentication policy named abc on the gateway and set the SSID to test.

```
FS# configure terminal
FS(config)# app-auth policy abc type qrcode
FS(app-auth-policy)# rule ssid test
```

Verification

Run the **show app-auth policy all** command to display the 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
```

Platform Description

This command is supported on gateway series products.

20.44 rule type pwd

Use this command to configure the account- and password-based authentication.

rule type pwd

Use the **no** form of this command to delete the account- and password-based authentication.

no rule type pwd

Parameter Description

Parameter	**Description**
pwd	Indicates account- and password-based authentication.

Defaults

N/A

Command Mode

APP-AUTH policy configuration mode

Default Level

14

Usage Guide

This command is available only in APP-AUTH policy group mode.

Configuration Example

#Configure an authentication policy named aaa and set the type to account- and password-based authentication.

```
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 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
```

Platform Description

This command is supported on gateway series products.

20.45 show app-auth auth-rule

Use this command to display IP addresses of an authenticated network segment.

show app-auth auth-rule

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Global configuration mode and privileged EXEC mode

Default Level 14

Usage Guide Use this command to display IP addresses of an authenticated network segment.

Configuration Example #Display IP addresses of an authenticated network segment.

```
FS#show app-auth auth-rule
auth rule ip:
            192.168.1.1 - 192.168.1.255
```

20.46 show app-auth deny-mac

Use this command to display denied MAC addresses.

show app-auth deny-mac

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Global configuration mode and privileged EXEC mode

Default Level 14

Usage Guide Use this command to display denied intranet MAC addresses.

Configuration Example #Display denied intranet MAC addresses.

```
FS#show app-auth deny-mac
app-auth deny-mac num: 1
            mac: 0010.1144.3344, flag: 1
```

Platform Description This command is supported only on gateway series products.

20.47 show app-auth direct-dstip

Use this command to display authentication-free extranet IP addresses.

show app-auth direct-dstip

Parameter Description

Parameter	**Description**
N/A	N/A

Command Global configuration mode and privileged EXEC mode

Mode

Default Level 14

Usage Guide Use this command to display authentication-free extranet IP addresses.

Configuration Example #Display authentication-free extranet IP addresses.

```
FS(config)#show app-auth direct-dstip
direct dst-ip:
        192.168.5.120
        1.1.1.1
```

Platform Description This command is supported only on gateway series products.

20.48 show app-auth direct-mac

Use this command to display authentication-free MAC addresses.

show app-auth direct-mac

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Global configuration mode and privileged EXEC mode

Default Level 14

Usage Guide Use this command to display authentication-free intranet MAC addresses.

Configuration Example #Display authentication-free intranet MAC addresses.

```
FS#show app-auth direct-mac
app-auth deny-mac num: 0
        mac: 0010.1144.3344, flag: 0
```

20.49 show app-auth direct-srcip

Use this command to display authentication-free intranet IP addresses.

show app-auth direct-srcip

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Global configuration mode and privileged EXEC mode

Default Level 14

Usage Guide Use this command to configure authentication-free intranet IP addresses.

Configuration Example #Display authentication-free intranet IP addresses.

```
FS(config)#show app-auth direct-srcip
direct src-ip:
          192.168.5.120
          1.1.1.1
```

20.50 show app-auth direct-url

Use this command to display authentication-free extranet URLs.

show app-auth direct-url

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Global configuration mode and privileged EXEC mode

Default Level 14

Usage Guide Use this command to configure authentication-free extranet URLs.

Configuration Example #Display authentication-free extranet URLs.

```
FS#show app-auth direct-url
direct url:
          www.baidu.com
```

Platform Description This command is supported only on gateway series products.

20.51 show app-auth local-auth config

Use this command to display parameters related to local authentication.

show app-auth local-auth config

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode and global configuration mode

Default Level

14

Usage Guide

Use this command to display parameter configuration related to local authentication on the device.

Configuration Example

#Display the configuration of local authentication.

```
FS# show app-auth local-auth config
enable: False
data-store-enable: True
data-store-age-day: 36
user-mac-limit: 0
online-time: 1
authorize-time: 33
restrict-range information:
  mobile:
    global: false
    name:
    state:    Idle
  pc:
    global: false
    name:
    state:    Idle
```

Field description:

Field	Description
enable	Whether the function is enabled
data-store-enable	Whether the user data is stored to the storage medium
data-store-age-day	Aging time of user data
user-mac-limit	Number of MAC addresses allowed for each user
online-time	Allowable online duration of a user who is successfully authenticated
authorize-time	Allowable online duration of an authorized user who is successfully authenticated
restrict-range information	Policy for restricting clients from Internet access
mobile	Mobile client user
pc	PC user
global	Whether local authentication is enabled globally

name	Time object name
state	Whether the policy takes effect

Platform Description This command is supported on gateway series products.

20.52 show app-auth local-auth subs

Use this command to display information about locally authenticated users.

show app-auth local-auth subs { **all** | **by-mac** *mac-address* | **by-name** *name-string* }

Parameter Description

Parameter	Description
all	Indicates all users.
by-mac	Displays users by MAC address.
mac-address	Indicates the MAC address of a user.
by-name	Displays users by username.
name-string	Indicates the username.

Command Mode Privileged EXEC mode and global configuration mode

Default Level 14

Usage Guide Use this command to display locally authenticated users on the device.

Configuration Example #Display information about the locally authenticated user named bbb.

```
FS# show app-auth local-auth subs by-name bbb
------------------------------------------------------------------------------------------
Name                                                            Mac_num Type     source   Mode
        Mac                Auto/Manual terminal    time
------------------------------------------------------------------------------------------
bbb                                                             1         local     pwd       manual
 |---- aabb.1111.2222    manual        mobile        2018-5-6 17:21:39
```

Field description:

Field	Description
Name	Username
Mac num	Number of MAC addresses
Type	User type
Source	User authentication source
Mode	User information generation mode

Mac	MAC address of the client
Auto/manual	Client information generation mode
Terminal	Client type
Time	Last time the MAC address is used

Platform Description

This command is supported on gateway series products.

20.53 show app-auth local-auth vip-group

Use this command to display information about VIP users who are locally authenticated.

show app-auth local-auth vip-group { **all** | **by-name** *name-string* }

Parameter Description

Parameter	Description
all	Indicates all users.
by-name	Displays users by username.
name-string	Indicates the username.

Command Mode

Privileged EXEC mode and global configuration mode

Default Level

14

Usage Guide

Use this command to display information about VIP users who are locally authenticated on the device.

Configuration Example

#Display information about all VIP users.

```
FS#show app-auth local-auth vip-group all
cnt: 1/100. ad_any_vip: 0
Group-name                                                    type       idx
--------------------------------------------------------------------------------
aaa                                                           local      0
```

Field description:

Field	Description
Cnt	Number of current user groups
Ad_any_vip	Whether VIP users are effective on AD domain users
Group-name	Name of a user group
Type	Type of the user group
Idx	Index of the user group

Platform Description

This command is supported on gateway series products.

20.54 show app-auth local-online

Use this command to display information about online users who are locally authenticated.

show app-auth local-auth { [**all** | **by-name** *name-str*] **from** *num1* **to** *num2* | **by-ip** *ip-address* }

Parameter Description

Parameter	Description
all	Displays all users.
by-name	Displays users by username.
name-str	Indicates the username.
from	Specifies the No. of the start record.
num1	Indicates the offset of the start record.
to	Specifies the No. of the end record.
num2	Indicates the offset of the end user record.
by-ip	Displays users by IP address.

Command Mode

Privileged EXEC mode and global configuration mode

Default Level

14

Usage Guide

Use this command to display information about online users who are locally authenticated on the device.

Configuration Example

#Display information about online users who are locally authenticated.

```
FS# show app-auth local-online all from    1 to 1
{ "code": 0, "msg": "OK", "data": { "total": 1, "online": [ { "name": "haha", "ip": "192.168.234.228", "mac": "001a.a91f.e7a0",
"type": "pwd", "time": "3118-9-28 16:29:46" } ] } }
```

Field description:

Field	Description
Code	Status code
Msg	Prompt
Data	Data
Total	Total number of users
Online	Number of online users
name	Username
Ip	User IP address
Mac	User MAC address
Type	Authentication type
Time	Authentication time

Platform Description

This command is supported on gateway series products.

20.55 show app-auth policy

Use this command to display an authentication policy.

show app-auth policy [**all** | **by-name** *name-string*]

Parameter Description

Parameter	Description
all	Displays all policies.
by-name	Displays policies by name.
name-string	Indicates a policy name.

Command Mode

Privileged EXEC mode and global configuration mode

Default Level

14

Usage Guide

Use this command to display information about authentication policies on the device.

Configuration Example

#Display details about all authentication policies.

```
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: Authentication policy 1
   enable: True
   pid: 1
   mode: pwd
   state: 0
   ip-range number: 1
   cfile-path: plcy1.php
   pwd: 0
   sms: 1
   qrcode-alone: 1
   qrcode-authorize: 1
   act-directory: 1
```

```
  weixin: 1
ip-range info:
      1. ALL
  server number 5:
      1. name: WeChat server         type: weixin
      2. name: QR code scanning server         type: qrcode-authorize
      3. name: Self-help QR code scanning server         type: qrcode-alone
      4. name: AD domain server         type: act-directory
      5. name: SMS server         type: sms
```

Field description:

Field	Description
Global information	Policy information
policy_cnt	Number of policies
Global Ip-range	Network segment in which a policy is effective
Detail	Policy details
Policy	Policy name
enable	Whether a policy is enabled
pid	Policy ID
mode	Policy mode
state	Policy status
ip-range number	Number of network segments in which a policy is effective
cfile-path	Policy parameter file
pwd	Number of associated local account- and password-based authentication servers
sms	Number of associated SMS-based authentication servers
qrcode-alone	Number of associated self-help QR code scanning servers
act-directory	Number of associated AD domain servers
weixin	Number of associated WeChat servers
ip-range info	Specific information about the network segment in which a policy is effective
server number	Server information

Platform Description

This command is supported on gateway series products.

20.56 show app-auth hz-info

Use this command to display site ID and site name information.

show app-auth hz-info

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide Use this command to display site ID and site name information if a server requires the site ID and site name information.

Configuration Example N/A

20.57 show app-auth proxy-url

Use this command to display proxy URL information.

show app-auth proxy-url

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide Use this command to display proxy URL information.

Configuration Example

20.58 show app-auth ssid-cfg

Use this command to display network segment and SSID information.

show app-auth ssid-cfg

Parameter Description

Parameter	Description
N/A	N/A

Command Privileged EXEC mode, global configuration mode, and interface configuration mode

Mode

Default Level 14

Usage Guide Use this command to display network segment and SSID information if a server requires the SSID information.

Configuration Example

Platform Description This command is supported only on gateway series products.

20.59 show app-auth statistics

Use this command to display all configurations related to application authentication.

show app-auth statistics

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide Use this command to display all configurations related to application authentication. This command is provided for web calling.

Configuration Example #Display all configurations related to application authentication.

```
FS# show app-auth statistics
```

20.60 show app-auth tcp-info

Use this command to display configurations related to a TCP keepalive connection.

show app-auth tcp-info

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide Use this command to display configurations related to a TCP keepalive connection.

Configuration Example #Display configurations related to a TCP keepalive connection.

```
FS#show app-auth tcp-info
tcp_server_url:
tcp_enable: 1
tcp_keepalive_period: 300
user_inform_period: 300
tcp_sock: -1
tcp_state: 1
server_ip: 0.0.0.0, port: 0
server_change: 1
rcv_pkt_num: 0
rcv_error_pkt_num: 0
keepalive_last_send_time: 0
keepalive_last_rcv_time: 0
user_inform_last_send_time: 0
user_inform_last_rcv_time: 0
```

20.61 show app-auth user

Use this command to display all online nodes that pass application authentication.

show app-auth user {**all** | **online** | **by-ip** *ip-addr* | **by-name** *name*}

Parameter Description

Parameter	Description
all	Displays all user information.
online	Displays online user information.
by-ip	Queries users by IP address.
ip-addr	Specifies an IP address.
by-name	Queries users by username.
name	Indicates a username.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide Use this command to display all online nodes that pass application authentication.

Configuration Example #Display online nodes.

```
FS# show app-auth online
ip          mac            status
```

ip: Indicates an IP address.

mac: Indicates a MAC address.

status: Indicates the state of a node: effective or ineffective.

app-id: Indicates a type of application to perform authentication.

Platform Description

This command is supported only on gateway series products.

20.62 show app-auth proxy-option config

Use this command to display HTTPS redirection information.

show app-auth proxy-option config

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

Use this command to display HTTPS redirection information.

Configuration Example

```
FS#show app-auth proxy-option config
---------- App-Auth Option Config Info ----------
Redirect for https     : Enable
Session total limit : 20001
Session per-ip limit: 201
---------------------- End ---------------------
FS#
```

Redirect for https: Enables HTTPS redirection.

Session total limit: Indicates a limit on the total number of HTTPS connections.

Session per-ip limit: Indicates a limit on the number of HTTPS connections per IP address.

Platform Description

This command is supported only on gateway series products.

21 Webservice Commands

21.1 webservice monitor-addr

Use this command to configure an IP address of a monitoring server.

webservice monitor-addr *url* **{ ip-range** *ip-start ip-end*}

Use the **no** form of this command to delete an IP address of a monitoring server.

no webservice monitor-addr *url* **{ ip-range** *ip-start ip-end* **}**

Parameter Description

Parameter	Description
url	Specifies a URL of a monitoring server.
ip-start	Specifies a start IP address.
ip-end	Specifies an end IP address.

Defaults

No IP address of a monitoring server is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

Use this command to configure an IP address of a monitoring server. User information will be pushed to the monitoring server after users go online if the server is connected to an HZ portal.

Configuration Example

N/A

Verification

Run the **show webservice hz-info** command to display the configuration result.

```
FS#show webservice hz-info
{"root":{"monitor-addr":"http://202.80.193.155:8090/"}, "branch": []}
```

Platform Description

This command is supported only on gateway series products.

21.2 webservice portal-check

Use this command to configure portal detection.

webservice portal-check [enable | interval *time_1* **| retransmit** *num***]**

Use the **no** form of this command to delete configurations related to portal detection.

no webservice portal-check [enable | interval | restransmit]

Parameter Description

Parameter	Description
enable	Enables portal detection.
interval	Specifies a detection interval. The default value is 30 seconds.
time_1	Specifies a detection period in seconds. The default value is 30 seconds.

retransmit	Specifies the maximum number of retransmission times in case of failure.
num	Specifies the number of retransmission times. The default value is 3

Defaults Portal detection is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide

1. Use this command to detect whether a server is normal. If not, APP-AUTH will be disabled. After the server recovers from an exception, APP-AUTH will be automatically enabled.
2. Ensure that the server supports this function before it is enabled.

Configuration Example N/A

Verification Run the **show webservcie config** command to display the configuration result.

```
FS#show webservice config
service-url:
sec-service-url:
webs-online: 0
webs-tmponline: 1
redirect_302: 1
portal-check: on
portal-check retransmit: 3
portal-check interval: 30

portal-ping: on
portal-ping retransmit: 1
portal-ping interval: 300

client-sync: off
client-sync intveral: 30

get_wanip_enable: on
get_wanip_interval: 120
webs_sin_ip: 0.0.0.0
wx_auth_enable: 0
wx_auth intveral: 72000
```

21.3 webservice service-url

Use this command to set a server URL.

webservice service-url *url*

Use the **no** form of this command to delete a server URL.

no webservice service-url

Parameter Description

Parameter	**Description**
url	Specifies a server URL.

Defaults No server URL is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to set a server URL if the gateway authentication protocol is set to WiFiDog or WiFi connection over WeChat and the server is connected to a WMC/MCP.

Configuration Example N/A

Verification Run the **show webservcie config** command to display the configuration result.

Platform Description This command is supported only on gateway series products.

21.4 webservice sec-service-url

Use this command to set a second URL of the server.

webservice sec-service-url *url*

Use the **no** form of this command to delete a server URL.

no webservice sec-service-url

Parameter Description

Parameter	**Description**
url	Specifies a server URL.

Defaults No second server URL is configured by default.

Command Mode Global configuration mode

Usage Guide Use this command to set a server URL if authentication is based on WiFi connection over WeChat and short messages and the server is connected to a WMC/MCP. The webserver-url is set to a URL of WiFi connection over WeChat, and webservice sec-service-url is set to a URL of WiFi connection over WiFiDog.

Configuration Example N/A

Verification Run the **show webservcie config** command to display the configuration result.

21.5 webservice monitor fmt

Use this command to configure the monitoring server type.

webservice monitor fmt *xwc*

Use the **no** form of this command to restore the default setting.

no webservice monitor fmt

Parameter Description

Parameter	Description
xwc	Specifies the monitoring server type to be Pronetway.

Defaults By default, no monitoring server type is configured.

Command Mode Global configuration mode

Default Level 14

Usage Guide Use this command to configure the monitoring server type. User information will be pushed to the monitoring server after users go online.

Configuration Example N/A

Verification Run the **show run | i monitor fmt** command to display the configuration result.

```
FS# show run | i monitor fmt
webservice monitor fmt xwc
```

Platform Description This command is supported only on gateway series products.

22 ANTI-PAP Commands

22.1 anti-pap avoid-block

Use this command to add the blocking-free server resources. Use the **no** or **default** form of this command to restore the default settings.

anti-pap avoid-block ip-group *id*

no anti-pap avoid-block ip-group *id*

default anti-pap avoid-block

Parameter Description

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

The command should be run to avoid blocking when internal clients visit the auth server and other special resources through devices.

Configuration Examples

The following example adds the blocking-free server.

```
FS(config)# anti-pap avoid-block ip-group 1
```

Related Commands

Command	Description
show anti-pap config	Displays the confiugration.

Platform Description

N/A

22.2 anti-pap control

Use this command to block the user for the specified period.

anti-pap control *addr* [*time*] { **block** | **limit down** *rate1* **up** *rate2*] } **base** { **user** | **ip** }

Parameter Description

Parameter	Description
addr	IP address of the user
time	Block time, range: 1-1440 minutes. Default time: 10 minutes.
user	Indicates blocking by username.
ip	Indicates blocking by IP address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example blocks the user for 20 minutes based on the username.

```
FS# anti-pap control 192.168.1.2 20 block base user
```

Related Commands

Command	Description
N/A	

Platform Description

N/A

22.3 anti-pap monitor

Use this command to detect the user, specify/update the device, and whether to block. Use the **no** or **default** form of this command to restore the default settings.

anti-pap monitor { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } [**expected-terminal pc**] [{ **block** [*time*] | **limit** [*time*] **down** *rate1* **up** *rate2* } **base** { **user** | **ip** }]

no anti-pap monitor [**subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** }]

default anti-pap monitor

Parameter Description

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-subscriber any	Specifies that all authenticated users will be detected.
expected-terminal pc	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** minutes. The default value is **10** minutes.
limit	Indicates the user bandwidth limit. The rate is not limited by default.
rate1	Indicates the downlink bandwidth, range 1-1000 Kbps.
rate2	Indicates the uplink bandwidth, range 1-1000 Kbps.
user	Indicates blocking by username.
ip	Indicates blocking by IP address.

Defaults

No user is detected.

Command

Global configuration mode

Mode

Usage Guide The username commonly is the 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.

Configuration Examples The following example detects all authenticated users whose expected client type is PC. If any AP is detected, the user will be blocked.

```
FS(config)# anti-pap monitor auth-subscriber any expected-terminal pc block
```

Related Commands

Command	Description
show anti-pap config	Displays the configuration.

Platform Description N/A

22.4 clear anti-pap control

Use this command to remove the user blocking.

clear anti-pap control *addr*

Parameter Description

Parameter	Description
addr	Indicates the IP address of user.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example removes the user blocking.

```
FS# clear anti-pap control 192.168.1.4
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

22.5 show anti-pap config

Use this command to display the blocking-free server and the user configuration.

show anti-pap config

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode or global configuration mode

Default Level

14

Usage Guide

Configuration Example

The following example displays the configuration information.

```
FS# show anti-pap config
{
    "code": 0,
    "msg": "",
    "data": {
        "avoid-block": [
            1
        ],
        "monitor": [
            {
                "User": "any",
                "Auth": "no",
                "Invalid": false,
                "Exp-Term": "any",
                "Ctrl": "block",
                "Time": 10,
                "ByUser": false
            }
        ]
    }
}
```

Field	Description
avoid-block	Blocking-free server resources
User	Username

Auth	Authenticated user or not
Invalid	Valid or invalid
Exp-Term	Expected device type: any-all device types PC-PC
Ctrl	Punishment type: Blank-no punishment block-blocking limit-limit the speed
Time	Period
ByUser	Block by username. False indicates blocking by IP address

Verification

22.6 show anti-pap log

Use this command to display the log.

show anti-pap log detail 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*]

Use this command to display the log quantity.

show anti-pap log stat from *y1 m1 d1* [*H1:M1:S1*] **to** *y2 m2 d2* [*H2:M2:S2*] [**subscriber** *subs-name1* | **auth-subscriber** *subs-name2*] [**ip** *addr*]

Parameter Description

Parameter	Description
y1 m1 d1	Start date
H1:M1:S1	Start time, default: 00:00:00
y2 m2 d2	End date
H2:M2:S2	End time, default: 23:59:59
subscriber *subs-name1* | **auth-subscriber** *subs-name2*	Local or authenticated username. No username is configured by default.
ip *addr*	IP address. Separate multiple IPs by comma. No IP is configured by default.
time	Sort the search result by time
subscriber	Sort the search result by local username
auth-subscriber	Sort the search result by authenticated username
ip	Sort the search result by IP address
asc	Sort the search result in ascending order
desc	Sort the search result in descending order
start-item *num1* **end-item** *num2*	Start and end position of search. All records are searched by default.

Command Global configuration mode or priviledge EXEC mode

Mode

Usage Guide N/A

Configuration Examples The following example displays the log.

```
FS# show anti-pap log from 2016-10-11 0:0:0 to 2016-10-11 23:59:59 order-by time desc start-item 1 end-item 20
{
    "code": 0,
    "msg": "",
    "data": [
        {
            "IP": "192.168.203.8",
            "User": "pc4",
            "Auth": false,
            "Manual": false,
            "Time": "2017-02-16 11:38:39",
            "Reason": [
                "PC",
                "Mobile"
            ],
            "Ctrl": "block"
        }
    ]
}
```

Field	Description
IP	IP address of user
User	Username
Auth	Authenticated user or not
Manual	Manual punishment or not
Time	Log generation time, that is, punishment time
Ctrl	Punishment type: Blank-no punishment block-blocking limit-limit the speed
Reason	Punishment reason and device information: PC-one PC is detected PC*-multiple PCs are detected Mobile-one mobile client is detected

	Mobile*-multiple mobile clients are detected VID-logged virtual accounts exceed the limit

Related Commands

Command	Description
N/A	

Platform Description

N/A

22.7 show anti-pap user

Use this command to display the user detection information.

show anti-pap user [**normal** | **controlled** | **subscriber** *subs-name1* | **auth-subscriber** *subs-name2* | **ip** *addr*]

Parameter Description

Parameter	Description
normal	Configure the search users as normal users.
controlled	Configure the search users as illegal users.
subscriber *subs-name1* | **auth-subscriber** *subs-name2*	Configure the local/authenticated username.
ip *addr*	Configure the IP address of users.

Defaults

None

Command Mode

Global configuration mode or priviledge EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the detection information of users.

```
FS# show anti-pap user

{

    "code": 0,

    "msg": "",

    "data": [

        {

            "IP": "192.168.203.6",

            "User": "pc4",

            "Auth": false,

            "Controlled": false,

            "Ctrl": "block"
        },
        {
            "IP": "192.168.203.5",
            "User": "pc4",
            "Auth": false,
            "Controlled": true,
            "Manual": false,
            "Time": "2017-02-16 11:36:33",
            "Reason": [
                "PC",
                "Mobile"
            ],
            "Ctrl": ""
        }
    ]
}
```

Field	Description
IP	IP address of user
User	Username
Auth	Authenticated user or not
Controlled	Punish or not
Manual	Manual punishment or not
Ctrl	Punishment type: Blank-no punishment block-blocking limit-limit the speed
Time	Update time of Reason field
Reason	Punishment reason, and device information: PC-one PC is detected PC*-multiple PCs are detected Mobile-one mobile client is detected Mobile*-multiple mobile clients are detected VID-logged virtual accounts exceed the limit

Related Commands

Command	**Description**
N/A	

Platform N/A

Description

23 WEB-ADVERT Commands

23.1 advertising enable

Use this command to enable the advertisement function in global configuration mode. This command is compatible with the **advertising webauth-free-user** command.

advertising enable

Use the **no** form of this command to disable the advertisement function.

no advertising enable

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults The advertisement function is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide You must configure the network segment range for advertisement push and the URL of an advertisement pop-up box so that the advertisement function is successfully applied.

Configuration Example #Enable the advertisement function.

```
FS(config)# advertising enable
```

Verification Run the **show advertising** command to display the configuration.

23.2 advertising free-user

Use this command to configure a network segment range for advertisement push. This command is compatible with the **webauth-free-user address <** *ip-address* **> mask <** *ip-mask***>** command.

advertising free-user ip < *ip-address* > **mask** < *ip-mask* >

Use the **no** form of this command to delete a network segment range.

no advertising free-user ip < *ip-address* > **mask** < *ip-mask* >

Parameter Description

Parameter	**Description**
ip-address	Indicates the IP address, in dotted decimal notation.
ip-mask	Indicates the subnet mask, in dotted decimal notation.

Defaults No network segment range for advertisement push is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide A maximum of 50 network segments can be configured.

Configuration Example

1. Configure a network segment for advertisement push.

```
FS(config)# advertising free-user ip 192.168.198.1 mask 255.255.255.0
```

2. Configure the full network segment for advertisement push. This command is compatible with the **advertising all-user without-webauth** command.

```
FS(config)# advertising free-user ip 0.0.0.0 mask 255.255.255.255
```

Verification N/A

23.3 advertising min-interval

Use this command to configure the periodical interception interval.

advertising min-interval *interval-value*

Use the **no** form of this command to delete the periodical interception interval.

no advertising min-interval

Parameter Description

Parameter	Description
interval-value	Indicates the interval in minutes. The value range is from 30 to 1440. The default value is 30.

Defaults The default periodical interception interval is 30 minutes.

Command Mode Global configuration mode

Default Level 14

Usage Guide

1. When periodical interception is disabled, the default value is **0**.
2. After periodical interception is enabled, the default value is **30**.
3. After periodical interception is enabled, an error occurs if the configured interval is deleted.

Configuration Example #Configure the periodical interception interval.

```
FS(config)# advertising min-interval 30
```

Verification Run the **show advertising** command to display the configuration.

23.4 advertising popup-page

Use this command to enable the function of preventing advertisement pop-up boxes from being intercepted by the browser. This command is compatible with the **web-auth advert popup-page** command.

advertising popup-page

Use the **no** form of this command to disable the function of preventing advertisement pop-up boxes from being intercepted by the browser.

no advertising popup-page

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is not configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is hidden. Therefore, it does not support the abbreviated mode.

Configuration Example #Enable the function of preventing advertisement pop-up boxes from being intercepted by the browser.

```
FS(config)# advertising popup-page
```

Verification Run the **show advertising** command to display the configuration.

23.5 advertising suppress

Use this command to enable periodical interception.

advertising suppress

Use the **no** form of this command to disable periodical interception.

no advertising suppress

Parameter Description

Parameter	Description
N/A	N/A

Defaults Periodical interception is disabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide The default periodical interception interval is 30 minutes after periodical interception is enabled.

Configuration Example #Enable periodical interception.

```
FS(config)# advertising suppress
```

Verification Run the **show advertising** command to display the configuration.

23.6 advertising url

Use this command to configure the URL of an advertisement pop-up box.

advertising url *url-string*

Use the **no** form of this command to delete the URL of an advertisement pop-up box.

no advertising url

Parameter Description

Parameter	Description
url-string	Indicates a URL. It must begin with "http://" "https://." Otherwise, a configuration failure prompt is displayed. The value contains a maximum of 255 characters.

Defaults No URL is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Example #Configure the URL of an advertisement pop-up box.

```
FS(config)# advertising url http://www.baidu.com/
```

Verification Run the **show advertising** command to display the configuration.

23.7 show advertising

Use this command to display basic configurations of the advertisement function.

show advertising

Parameter Description

Parameter	Description

N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command displays the basic parameter settings of the advertisement function.

Configuration Example #Display the basic configurations of the advertisement function.

```
FS#show advertising
advertising enable:             On
advertising url:                http://www.baidu.com/
advertising suppress:           On
advertising popup-page:         On
advertising min-interval: 30
advertising free-user:
    192.168.198.0      255.255.255.0
    1.1.1.1            255.255.0.0
```

Field description:

Field	Description
advertising popup-page	Displays the basic configurations only after the advertisement functior enabled.
advertising free-user	Displays the basic configurations only after a network segment range advertisement push is configured.

23.8 show advertising free-user

Use this command to display the network segment range for advertisement push. This command is compatible with the **show webauth-free-user** command.

show advertising free-user

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command displays the network segment range for advertisement push.

Configuration #Display the network segment range for advertisement push.

Example

```
FS#show advertising free-user
free-user configuration:
  Address              Mask
  --------------- ---------------
  192.168.198.0      255.255.255.0
  1.1.1.1            255.255.0.0
  2.2.2.2            255.0.0.0
```

Field description:

Field	Description
Address	Indicates an IP address.
Mask	Indicates the subnet mask of the IP address.

23.9 show advertising user

Use this command to display users who access the network through advertisement push. This command is compatible with the **show advertising tmo** command.

show advertising user

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command displays users who access the network through advertisement push.

Configuration Example

#Display users who access the network through advertisement push.

```
FS(config)#show adv user
Current online advertising user num: 1
Address              Online    Time Limit       Time used          Name
--------------- ------- -------------- -------------- ---------
192.168.198.34    On          0d 00:30:00       0d 00:08:50       AD_USER
```

Field	Description
Address	Indicates an IP address.
Online	Indicates whether a user is online.
Time Limit	Indicates the advertisement push interval.
Time used	Indicates the online duration.
Name	Indicates a username. The default username is **AD_USER**.

24 Local-Account Commands

24.1 debug local-account

Use this command to enable the debugging function. Use the **no** form of this command to disable the debugging function.

debug local-account { client *num* **| http_proxy | server }**

no debug local-account { client *num* **| http_proxy | server }**

Parameter Description

Parameter	Description
client	Enables the debugging function on the client.
num	Indicates the client number.
http_proxy	Enables the debugging function on the HTTP proxy.
server	Enables the debugging function on the server.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to display debugging information about this module.

Configuration Examples

The following example enables the debugging function on the server.

```
FS# debug local-account server
```

Prompt Message

The debugging function is enabled.

```
FS#show debug
debug:
  local account debug debugging is on

FS#
```

24.2 description

Use this command to configure a description for a user.

description *string*

Parameter Description

Parameter	Description
description *string*	Indicates the description of a user.

Defaults

No description is configured for a user by default.

Command Mode

local-account-user mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example configures a description for a user.

```
FS# configure terminal
FS(config)# local-account user test
FS(local-account-user)# description test
FS(local-account-user)# exit
FS(config)# end
```

Verification

Run the **show local-account users** command to display the user description.

```
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    2018/01/21
192.168.1.2            11:11:22:22:33:33      test

total:1        upper limit:150
FS
```

24.3 ip

Use this command to bind the user IP address.

ip *a.b.c.d*

Parameter Description

Parameter	Description
ip *a.b.c.d*	Indicates the IP address to be bound for a user.

Defaults

No IP address is bound for a user by default.

Command Mode

local-account-user mode

Default Level

14

Usage Guide

N/A

Configuration

The following example binds the IP address 192.168.1.2 for a user.

Examples

```
FS# configure terminal
FS(config)# local-account user test
FS(local-account-user)# ip 192.168.1.2
FS(local-account-user)# exit
FS(config)# end
```

Verification

Run the **show local-account users** command to display the bound user IP address. The IP address displayed in the **Ip addr** column is bound for the user.

```
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    2018/01/21
192.168.1.2            11:11:22:22:33:33      test

total:1        upper limit:150
FS
```

24.4 local-account user

Use this command to create a user.

local-account user *username*

Parameter Description

Parameter	Description
user *username*	Indicates the username.

Defaults

No user is configured by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example creates a user named test.

```
FS# configure terminal
FS(config)# local-account user test
FS(local-account-user)# exit
FS(config)# end
```

Verification

Run the **show local-account users** command to display the user status.

```
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    2018/01/21
192.168.1.2           11:11:22:22:33:33      test

total:1        upper limit:150
FS
```

24.5 local-account period

Use this command to configure the interval for the external module to send notifications.

local-account period *time*

Parameter Description

Parameter	Description
period *time*	Indicates the interval for the external module to send notifications.

Defaults No interval is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example sets the notification interval to 60s.

```
FS# configure terminal
FS(config)# local-account period 60
FS(config)# end
```

Verification Run the **show local-account config** command to display the user status.

```
FS#show local-account config
users-limit: 150
acct-period: 60s
notice: on
notice-time: 5h
notice-interval: 10m
FS
```

24.6 local-account notice

Use this command to configure a user notification system.

local-account notice { enable | date-rule *hour interval-min* **}**

Parameter Description

Parameter	Description
notice	Indicates the user notification system.
enable	Enables user notification.
date-rule	Sets date rules for notifications.
hour	Indicates the time in advance users are notified that their accounts are about to expire.
interval-min	Indicates the notification interval.

Defaults No user notification system is configured by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide N/A

Configuration Examples The following example enables the notification function and configures the device to give notifications 5 hours before expiration and at an interval of 10 minutes.

```
FS# configure terminal
FS(config)# local-account notice enable
FS(config)# local-account notice date-rule 5 10
FS(config)# end
```

Verification Run the **show local-account config** command to display the user status.

```
FS#show local-account config
users-limit: 150
acct-period: 20s
notice: on
notice-time: 5h
notice-interval: 10m
FS
```

24.7 mac

Use this command to bind the user MAC address.

mac { *mac-address* | **auto** }

Parameter

Parameter	Description

Description

mac	Binds the MAC address.
mac-address	Indicates manual MAC address binding.
auto	Indicates automatic MAC address binding.

Defaults

No MAC address is bound for a user by default.

Command Mode

Local-account-user mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example binds the MAC address of a user.

```
FS# configure terminal
FS(config)# local-account user test
FS(local-account-user)# mac 1111.2222.3333
FS(local-account-user)# exit
FS(config)# end
```

Verification

Run the **show local-account config** command to display the user status.

```
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    2018/01/21
192.168.1.2             11:11:22:22:33:33      test

total:1        upper limit:150
FS
```

24.8 policy

Use this command to configure a charging policy for users.

policy date *yyyy mm dd*

Parameter Description

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.

Defaults

No charging policy is configured by default.

Command Mode

local-account-user mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example configures a charging policy, in which the expiration date is December 12, 2020.

```
FS# configure terminal
FS(config)# local-account user test
FS(local-account-user)# policy date 2020 12 12
FS(local-account-user)# exit
FS(config)# end
```

Verification

Run the **show local-account users** command to display the user status.

```
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   2020/12/12
192.168.1.2         11:11:22:22:33:33     test

total:1        upper limit:150
FS
```

24.9 show local-account config

Use this command to display the configuration of this module.

show local-account config

Parameter Description

Parameter	Description
config	Displays the configuration and parameters of the module.

Defaults

N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

N/A

Configuration Examples

N/A

Verification

Run the **show local-account config** command to display the configuration of this module.

```
FS# show local-account config
users-limit: 150
acct-period: 20s
notice: on
notice-time: 48h
notice-interval: 60m
FS#
```

Field description:

Field	Description
lacc	Whether the local charging function is enabled
users-limit	Maximum number of supported users
acct-period	Interval for the external module to send notifications, in seconds
notice	Whether to enable the user notification system when user accounts are about to expire
notice-time	Time in advance users are notified that their accounts are about to expire
notice-interval	Notification interval

24.10 show local-account online

Use this command to display information about online users.

show local-account online [**by-name** *name*]

Parameter Description

Parameter	Description
online	Displays online users.
by-name	Searches for users by username.
name	Indicates the username.

Defaults

N/A

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide N/A

Configuration Examples N/A

Verification Run the **show local-account online by-name test1** command to check whether the user is online.

```
FS#show local-account online by-name test1


-------------------------------------------------------------------------------------------
Name              Ip addr              Mac addr               Start                   Online
-------------------------------------------------------------------------------------------
test1          192.168.0.13       00:23:24:03:03:03    2018/01/22 14:06:43    0days 00:02:55


Total:1
FS#
```

Field description:

Field	Description
Name	Username
Ip addr	IP address of the user
Mac addr	MAC address of the user
Start	Time when the user goes online
Online	Online duration
Total	Number of users under this account

24.11 show local-account users

Use this command to display user information.

show local-account users [**by-name** *name*]

Parameter Description

Parameter	Description
users	Displays users.
by-name	Searches for users by username.
name	Username

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide N/A

Configuration Examples N/A

Verification Run the **show local-account users** command to display user information.

```
FS# show local-account users

(O) Online    (S) State: 0=Invalid 1=Normal 3=Overdue
-----------------------------------------------------------------------------------------------
Name                   O   S   Policy          Ip addr                  Mac addr                  Note
-----------------------------------------------------------------------------------------------
test1                0   1   N/A              N/A                        N/A                          testtest

Total:1       Upper limit:150
FS#
```

Field description:

Field	Description
Name	Username
O	Online, indicating that the user is online
S	State, indicating the user status
Policy	Charging policy of the user
Ip addr	Whether the user IP address is bound
Mac addr	Whether the user MAC address is bound
Note	Remarks of the user
Total	Total number of current users
Upper limit	Total number of users supported by the system

25 Firewall Commands

25.1 NETWORK_DEFEND Commands

25.1.1 bypass

Use this command to configure a policy that allows bypass traffic to enter a network attack defense domain. Use the **no** form of this command to delete the configured policy that allows bypass traffic to enter a network attack defense domain. Use the **default** form of this command to restore the default settings.

bypass *src-ip-address* [**mask** *src-ip-mask*] [**proto** { **tcp** [**dest-port** *dest-port-num*] | **udp** [**dest-port** *dest-port-num*] | **icmp** | *protocol-num* }]

no bypass *src-ip-address* [**mask** *src-ip-mask*] [**proto** { **tcp** [**dest-port** *dest-port-num*] | **udp** [**dest-port** *dest-port-num*] | **icmp** | *protocol-num* }]

default bypass *src-ip-address* [**mask** *src-ip-mask*] [**proto** { **tcp** [**dest-port** *dest-port-num*] | **udp** [**dest-port** *dest-port-num*] | **icmp** | *protocol-num* }]

Parameter Description

Parameter	Description
src-ip-address	Indicates the source IP address.
src-ip-mask	Indicates the subnet mask of the source IP address.
tcp	Indicates the TCP protocol.
udp	Indicates the UDP protocol.
icmp	Indicates the ICMP protocol.
protocol-num	Indicates the protocol number.
dest-port-num	Indicates the destination port number.

Defaults

No policy that allows bypass traffic to enter a network attack defense domain is configured by default.

Command Mode

config-defend-zone configuration mode

Default Level

14

Usage Guide

Traffic matching a rule in the policy is considered as bypass traffic.

Configuration Examples

The following example configures a policy on the egress gateway or wireless AC, in which TCP packets (with the destination port of 80) from the host with the IP address of 192.168.9.2 are allowed to directly pass through the network attack defense domain named web.

```
FS(config)# defend-zone web
FS(config-defend-zone)# bypass 192.168.9.2 proto tcp dest-port 80
FS(config-defend-zone)# exit
```

Verification

Run the **show running** command to check whether a policy that allows bypass traffic to enter a network attack defense domain is configured successfully.

25.1.2 blacklist

Use this command to add a host to the blacklist to forbid the traffic of the host from entering or leaving a network attack defense domain. Use the **no** form of this command to delete a host from the blacklist. Use the **default** form of this command to restore the default settings.

blacklist *ip-address*

no blacklist [*ip-address*]

default blacklist [*ip-address*]

Parameter Description

Parameter	Description
ip-address	Indicates the IP address of the host to be blacklisted.

Defaults No host is added to the blacklist.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide This command is used to add a host to the blacklist to forbid the traffic of the host from entering or leaving a network attack defense domain.

Configuration Examples The following example forbids packets of the host with the IP address of 192.168.9.2 from passing through the network attack defense domain named web.

```
FS(config-defend-zone)# blacklist 192.168.9.2
FS(config-defend-zone)# exit
```

Verification Run the **show running** command to check whether the blacklist is configured successfully.

25.1.3 clear defend

Use this command to clear statistics on packet loss caused by attack defense.

clear defend drop

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to clear statistics on packet loss caused by attack defense.

Configuration Examples

The following example clears statistics on packet loss caused by attack defense.

```
FS# clear defend drop
```

25.1.4 clear defend-zone

Use this command to clear statistics of a network attack defense domain.

clear defend-zone *net-defend-zone-name* **counters**

Use this command to clear global protection statistics.

clear defend-zone global counters

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.
global	Indicates global protection.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to clear data transmission and receiving statistics as well as TopN list in traffic monitoring.

Configuration Examples

The following example clears statistics of the network attack defense domain named web.

```
FS# clear defend-zone web counters
```

25.1.5 defend

Use this command to enable the defense against specified protocol attacks. Use the **no** form of this command to disable the defense against specified protocol attacks. Use the **default** form of this command to restore the default settings.

defend { **winnuke | source-route | route-record | icmp-unreachable | fraggle | land | large-icmp** [*icmp-length*] }

no defend { **winnuke | source-route | route-record | icmp-unreachable | fraggle | land | large-icmp** }

default defend { **winnuke | source-route | route-record | icmp-unreachable | fraggle | land | large-icmp** }

Parameter Description

Parameter	Description
winnuke	Configures the defense against WinNuke attacks on the firewall. WinNuke attack packets will be discarded.
source-route	Configures the defense against source route attacks on the firewall. IP packets using this option will be discarded.
route-record	Configures the defense against route-record attacks on the firewall. IP packets using this option will be discarded.
icmp-unreachable	Configures the defense against ICMP destination unreachable attacks on the firewall. ICMP destination unreachable packets will be discarded.

fraggle	Configures the defense against Fraggle attacks on the firewall.
land	Configures the defense against LAND attacks on the firewall. IP packets with the source IP address same as the destination IP address will be discarded.
large-icmp	Configures the defense against jumbo ICMP packet attacks on the firewall.
icmp-length	Indicates the allowable ICMP packet length, in bytes. ICMP packets beyond this length will be discarded. The default value is 4,000 bytes. The value ranges from 28 to 65,499.

Defaults

The defense against LAND attacks is enabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

This command is used to enable the defense against various protocol attacks.

- The source IP address may be the same as the destination IP address in some special valid applications (such as BFD). In this case, the defense against LAND attacks needs to be disabled on the firewall.

Configuration Examples

The following example enables the defense against WinNuke attacks.

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# defend winnuke
```

Verification

1. Run the **show running** command to check whether the defense against protocol attacks is configured successfully.
2. Run the **show defend drop** command to display packet loss caused by the defense against protocol attacks.

25.1.6 defend-zone

Use this command to configure a network attack defense domain. Use the **no** form of this command to delete the network attack defense domain. Use the **default** form of this command to restore the default settings.

defend-zone *net-defend-zone-name*
no defend-zone *net-defend-zone-name*
default defend-zone *net-defend-zone-name*

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.

Defaults

No network attack defense domain is configured by default.

Command Mode

Global configuration mode

Default Level 14

Usage Guide Network attack defense domains can be configured on the device to provide independent protection measures and protection management for different protection objects. Each network attack defense domain contains at least two parts: a defined collection (associated with ACLs) of protected hosts and the protection policy.

If the network segment, to which a protected interface belongs, is large (for example, the subnet mask is about 16 bits), you need to configure an anti-scanning policy in the network attack defense domain in routing mode. The purpose is to prevent switch abnormalities caused by scanning attacks.

Configuration Examples N/A

Verification 1. Run the **show running** command to check whether a network attack defense domain is configured successfully.

2. Run the **show defend-zone** *net-defend-zone-name* command to display the status of the network attack defense domain.

25.1.7 defend-zone global

Use this command to enable global protection. Use the **no** form of this command to disable global protection. Use the **default** form of this command to restore the default settings.

defend-zone global

no defend-zone global

default defend-zone global

Parameter Description

Parameter	Description
N/A	N/A

Defaults Global protection is enabled by default.

Command Mode Global configuration mode

Default Level 14

Usage Guide Global protection can directly classify and limit all traffic of the current device. It can effectively defend against TCP flooding, and limit the rate of new UDP, ICMP and other protocol packets to restrict the UDP, ICMP, and other protocol attacks. The defense and rate limit can effectively enhance the firewall's defense capability against attacks and reduce network resources occupied by various flooding traffic.

Global protection is enabled by default. It needs to be disabled when the firewall performance and capacity are tested.

Configuration Examples The following example enables global protection.

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
```

```
FS(config)# defend-zone global
```

Verification

1. Run the **show running** command to check whether global protection is enabled successfully.
2. Run the **show defend drop** command to display packet loss caused by global protection.

25.1.8 description

Use this command to configure a description for a network attack defense domain. Use the **no** form of this command to delete the description of the network attack defense domain. Use the **default** form of this command to restore the default settings.

description *description-string*

no description

default description

Parameter Description

Parameter	Description
description-string	Indicates the description of a network attack defense domain. It can contain a maximum of 100 characters.

Defaults No description is configured by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide This command is used to configure a description for a network attack defense domain.

Configuration Examples

The following example configures a description for the network attack defense domain named web.

```
FS(config)#    defend-zone web
FS(config-defend-zone)# description “Defend policy for zone abc”
```

Verification Run the **show defend-zone** *net-defend-zone-name* command to display the description of the network attack defense domain.

25.1.9 detect

Use this command to configure the anti-scanning detection sensitivity, interval, and number of consecutive scans. Use the **no** form of this command to delete the configured anti-scanning detection sensitivity, interval, and number of consecutive scans. Use the **default** form of this command to restore the default settings.

detect { **low | medium | high** } { **period** *time-interval* | **times** *last-times* }

no detect { **low | medium | high** } { **period** | **times** }

default detect { **low | medium | high** } { **period** | **times** }

Parameter Description

Parameter	Description

low	Indicates detection at low sensitivity.
medium	Indicates detection at medium sensitivity.
high	Indicates detection at high sensitivity.
time-interval	Indicates the anti-scanning detection interval, in seconds. The value ranges from 1 to 2000.
last-times	Indicates the number of consecutive scans. It is considered that a scanning attack occurs only when the number of consecutive scans reaches this value. The value ranges from 1 to 10 and the default value is 1.

Defaults You can run the **show scan parameter** command to display default values of parameters and current parameter configuration. For field descriptions, see the **show scan parameter** command.

Command Mode config-scan-policy configuration mode

Default Level 14

Usage Guide This command is used to set the sensitivity for anti-scanning detection.

Configuration Examples The following example sets the low-sensitivity detection interval to 100 seconds.

```
FS(config)# scan policy
FS(config-scan-policy)# detect low period 100
```

Verification Run the **show scan parameter** command to display parameter results.

25.1.10 icmp auth-src-in

Use this command to configure a policy for defending against ICMP traffic from authentic source hosts. Use the **no** form of this command to **delete** the policy for defending against ICMP traffic from authentic source hosts. Use the **default** form of this command to restore the default settings.

icmp auth-src-in src-ip threshold *threshold-num* [**timeout** *seconds*] **action** { **limit | blocking | notify** }

no icmp auth-src-in src-ip

default icmp auth-src-in src-ip

Parameter Description

Parameter	Description
auth-src-in	Indicates packets that enter a network attack defense domain and are from authentic source hosts.
src-ip	Indicates that the policy is applied to identify packets from each source host.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
limit	Limits the traffic below the value of *threshold-num*.

blocking	Blocks the traffic of the host that enters and leaves the attack defense domain.
notify	Records the attack event only.

Defaults No such a policy is configured by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide When the rate of ICMP traffic that is from any authentic source host and enters a 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, or blocks all traffic of the source host that enters or leaves the network attack defense domain (according to the policy execution time). The policy execution duration is not shorter than the value of *seconds*.

Configuration Examples The following example configures a policy for defending against ICMP flood traffic from authentic source hosts for the network attack defense domain named web. In the policy, when the ICMP packets sent from a source host (passing source verification) to the network attack defense domain named web exceed 100 pps, the device is required to block all traffic of the host (for at least 60 seconds).

```
FS(config)# defend-zone web
FS(config-defend-zone)# icmp auth-src-in src-ip threshold 100 action blocking FS(config-defend-zone)# exit
```

25.1.11 icmp pkt-in

Use this command to configure a policy for limiting the ICMP traffic that enters a network attack defense domain. Use the **no** form of this command to delete the policy for limiting the ICMP traffic that enters a network attack defense domain. Use the **default** form of this command to restore the default settings.

icmp pkt-in { **dst-ip | global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit | notify** }

no icmp pkt-in { **dst-ip |global** }

default icmp pkt-in { **dst-ip |global** }

Parameter Description

Parameter	Description
pkt-in	Indicates all types of packets that enter a network attack defense domain.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
dst-ip	Indicates that the policy is applied to identify packets sent to each destination host.
global	Indicates that the policy is applied to identify all packets that enter the domain.
limit	Limits the traffic below the value of *threshold-num*.
notify	Records the attack event only.

Defaults N/A

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide When the rate of ICMP traffic that enters a network attack defense domain exceeds the threshold, the device limits the rate of the traffic to be lower than or equal to the threshold. The policy execution duration is not shorter than the value of *seconds*.

When the rate of ICMP traffic destined for any host in a network attack defense domain exceeds the threshold, the device limits the rate of the traffic to be lower than or equal to the threshold. The policy execution duration is not shorter than the value of *seconds*.

Configuration Examples The following example configures a policy for defending against ICMP flood traffic for the network attack defense domain named web. In the policy, when the rate of ICMP packets destined for a host in the network attack defense domain named web exceeds 100 pps, the device is required to limit the ICMP traffic of the host (not exceeding 100 pps).

```
FS(config)# defend-zone web
FS(config-defend-zone)# icmp pkt-in dst-ip threshold 100 action limit
FS(config-defend-zone)# exit
```

25.1.12 icmp unauth-src-in

Use this command to configure a policy for defending against ICMP traffic that does not pass authentic source verification. Use the **no** form of this command to delete the policy for defending against ICMP traffic that does not pass authentic source verification. Use the **default** form of this command to restore the default settings.

icmp unauth-src-in { **dst-ip** | **global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit** | **drop | notify** }

no icmp unauth-src-in { **dst-ip** | **global** }

default icmp unauth-src-in { **dst-ip** | **global** }

Parameter Description

Parameter	Description
unauth-src-in	Indicates packets that enter a network attack defense domain but do not pass authentic source verification.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
dst-ip	Indicates that the policy is applied to identify packets sent to each destination host.
global	Indicates that the policy is applied to identify all packets that enter the domain.
limit	Limits the traffic below the value of *threshold-num*.
drop	Discards the traffic.
notify	Records the attack event only.

Defaults No such a policy is configured by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide When the rate of ICMP packets that enter a network attack defense domain but do not pass the authentic 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 or discards all such packets.

When the rate of ICMP packets that are destined for any host in a network attack defense domain but do not pass the authentic 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.

Configuration Examples The following example configures a policy for defending against ICMP flood packets using fake source IP addresses, for the network attack defense domain named web. In the policy, when the rate of ICMP packets using suspicious fake source IP addresses destined for a host in the network attack defense domain named web exceeds 100 pps, the device is required to limit such ICMP traffic (not exceeding 100 pps); when the attack is stopped, the policy will keep effective for 1 hour.

```
FS(config)# defend-zone web
FS(config-defend-zone)# icmp unauth-src-in global threshold 100 timeout 3600 action rate-limit
```

25.1.13 ignore

Use this command to ignore the scanning category during anti-scanning detection. Use the **no** form of this command to cancel ignoring the scanning category during anti-scanning detection. Use the **default** form of this command to restore the default settings.

ignore protocol { **tcp** | **udp** | **icmp** | **other-protocol** }

no ignore protocol { **tcp** | **udp** | **icmp** | **other-protocol** }

default ignore protocol { **tcp** | **udp** | **icmp** | **other-protocol** }

Parameter Description

Parameter	Description
icmp	Indicates the ICMP protocol.
other-protocol	Indicates protocols other than TCP, UDP, and ICMP.
tcp	Indicates the TCP protocol.
udp	Indicates the UDP protocol.

Defaults Anti-scanning detection is applied to all protocol categories.

Command Mode config-scan-policy configuration mode

Default Level 14

Usage Guide This command is used to ignore the scanning behavior of a protocol as required. This command can be configured multiple times.

Configuration Examples The following example ignores the scanning of the TCP protocol during anti-scanning detection.

```
FS(config)# scan policy
FS(config-scan-policy)# ignore protocol tcp
```

25.1.14 ip access-group

Use this command to configure an ACL to be associated with a network attack defense domain. Use the **no** form of this command to disassociate the ACL from the network attack defense domain. Use the **default** form of this command to restore the default settings.

ip access-group *access-list*

no ip access-group

default ip access-group

Parameter Description

Parameter	Description
access-list	Indicates the name of the associated IP-compliant ACL.

Defaults No ACL is associated with a network attack defense domain by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide This command is used to configure an ACL to be associated with a network defense domain, to define the protection area of the 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.

Configuration Examples The following example configures the network attack defense domain named web to protect all hosts (defined in the ACL server) in the 192.168.3.X network segment.

```
FS(config)# ip access-list standard server
FS(config-std-nal)#10 permit 192.168.3.0 0.0.0.255
FS(config-std-nal)#exit
FS(config)# defend-zone web
FS(config-defend-zone)# ip access-group server
FS(config-defend-zone)# exit
```

Verification Run the **show defend-zone** command to display the desired ACL and whether the ACL is correctly associated.

25.1.15 log

Use this command to enable the function of logging different types of attacks. Use the **no** form of this command to disable the function of logging different types of attacks. Use the **default** form of this command to restore the default settings.

log { **tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | all** } [**syslog** | **save**]

no log { **tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | all** } [**syslog** | **save**]

default log { **tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | all** } [**syslog** | **save**]

Parameter Description

Parameter	Description
tcp-auth	Logs all TCP attacks from authentic source IP addresses.
tcp-unauth	Logs all attacks using TCP traffic that does not pass authentic source verification.
Icmp	Logs all ICMP attacks.
udp	Logs all UDP attacks.
other-protocol	Logs all attacks of other protocols (except TCP, UDP, and ICMP).
scan	Logs scanning attacks.
all	Logs all types of attacks.
syslog	Records attack logs in the form of system logs.
save	Saves attack information to the database.

Defaults The attack logging function is disabled by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide This command is used to enable the function of logging different types of attacks. The keyword **all** indicates that all types of attacks are logged. When **syslog** or **save** is not carried in the command, attack information is both recorded in the system logs and database.

Configuration Examples The following example saves all ICMP attack logs.

```
FS(config)# defend-zone web

FS(config-defend-zone)# log icmp save

FS(config-defend-zone)# exit
```

Verification

After an attack occurs, run the **show defend-zone** *net-defend-zone-name* **report** command to display attack results.

25.1.16 net-defend enable

Use this command to enable NETWORK_DEFEND. Use the **no** form of this command to disable NETWORK_DEFEND. Use the **default** form of this command to restore the default settings.

net-defend enable

no net-defend enable

default net-defend enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

NETWORK_DEFEND is disabled by default.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

When you need to enable NETWORK_DEFEND, you must also enable 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.

Configuration Examples

The following example enables NETWORK_DEFEND.

```
FS(config)# net-defend enable
```

Platform Description

Egress gateways support this command. NETWORK_DEFEND is enabled on firewalls by default and therefore, firewalls do not support this command.

25.1.17 net-defend learning

Use this command to enable defense policy self-learning in a network attack defense domain.

net-defend learning *net-defend-zone-name* [**days** *days*]

Use this command to enable defense policy self-learning for global protection.

net-defend learning global [**days** *days*]

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.
global	Indicates global protection.
days	Indicates the number of policy learning days.

Command

Privileged EXEC mode

Mode

Default Level 14

Usage Guide 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. During policy learning, the system automatically enables the session-based policy for defending against TCP SYN flooding attacks for the network attack defense domain, in which policy learning is started. 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.

Configuration Examples The following example enables policy learning for the network attack defense domain named web for 7 days.

```
FS(config)# defend-zone web
FS(config-defend-zone)#    ip access-group server
FS(config-defend-zone)# exit
FS# net-defend learning web
Net defend policies learning for defend-zone 'web' begin. (Period:    7 days)
```

Prompt Message 1. Policy learning is enabled successfully.

```
FS# net-defend learning web
Net defend policies learning for defend-zone 'web' begin. (Period:    7 days)
```

2. A defense policy is already available and policy learning cannot be enabled.

```
FS#net-defend learning web
Learning policy for 'web' fail: policies have been configured.
```

25.1.18 net-defend mode

Use this command to configure the NETWORK_DEFEND mode. Use the **no** form of this command to cancel the configured NETWORK_DEFEND mode. Use the **default** form of this command to restore the default settings.

net-defend mode { **nat** | **no-nat** }

no net-defend mode { **nat** | **no-nat** }

default i net-defend mode { **nat** | **no-nat** }

Parameter Description

Parameter	Description
nat	Indicates the NAT mode.
no-nat	Indicates the non-NAT mode.

Defaults The default NETWORK_DEFEND mode is NAT mode on gateways and non-NAT mode on bridges.

Command Mode Global configuration mode

Default Level 14

Usage Guide If NAT is deployed on the network, the NETWORK_DEFEND mode needs to be set to NAT mode. Bridges do not support NAT and the NAT mode cannot be configured on them.

Configuration Examples The following example sets the NETWORK_DEFEND mode to NAT mode.

```
FS(config)# net-defend mode nat
```

Platform Description Egress gateways support this command. Firewalls do not support NAT and therefore do not support this command.

25.1.19 ratelimit

Use this command to limit the bandwidth of traffic that enters or leaves a network attack defense domain. Use the **no** form of this command to cancel the limit on the bandwidth of traffic that enters or leaves a network attack defense domain. Use the **default** form of this command to restore the default settings.

ratelimit { **in** | **out** } [**src-ip** | **dst-ip**] **bandwidth** *bps-num*

no ratelimit { **in** | **out** } [**src-ip** | **dst-ip**]

default ratelimit { **in** | **out** } [**src-ip** | **dst-ip**]

Parameter Description

Parameter	**Description**
in	Limits the bandwidth of traffic that enters a network attack defense domain.
out	Limits the bandwidth of traffic that leaves a network attack defense domain.
src-ip	Applies the limit to each source IP address.
dst-ip	Applies the limit to each destination IP address.
bps-number	Indicates the bandwidth limit, in bps. The value ranges from 1 to 1,000,000,000.

Defaults No bandwidth limit is configured by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide **src-ip**: Limits the bandwidth of each source IP address.

dst-ip: Limits the bandwidth of each destination IP address.

✓ 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.

Configuration Examples

The following example limits the total bandwidth of traffic that enters the network attack defense domain named web to be no more than 100,000,000 bps.

```
FS(config)# defend-zone web
FS(config-defend-zone)# ratelimit in bandwidth 100000000
FS(config-defend-zone)# exit
```

25.1.20 session-limit

Global Protection

Use this command to limit the session creation rate. Use the **no** form of this command to cancel the limit on the session creation rate. Use the **default** form of this command to restore the default settings.

session-limit { **unauth-src-new-session | tcp | udp | icmp | other-protocol** } *new-session-per-second*

no session-limit { **unauth-src-new-session | tcp | udp | icmp | other-protocol** }

default session-limit { **unauth-src-new-session | tcp | udp | icmp | other-protocol** }

Attack Defense Domain

Use this command to limit the creation rate of sessions that enter or leave a network attack defense domain. Use the **no** form of this command to cancel the limit on the session creation rate. Use the **default** form of this command to restore the default settings.

session-limit { in | out } [src-ip | dst-ip] session-rate *new-session-per-second*

no session-limit { in | out } [src-ip | dst-ip]

default session-limit { in | out } [src-ip | dst-ip]

Parameter Description

Parameter	Description
new-session-per-second	Indicates the number of sessions to be created per second. The value ranges from 1 to 1,000,000.
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 TCP, UDP, and ICMP sessions.
in	Limits the creation rate of sessions that enter the network attack defense domain.
out	Limits the creation rate of sessions that leave the network attack defense domain.
src-ip	Applies the limit to each source IP address.
dst-ip	Applies the limit to each destination IP address.

Defaults

The default values of the **session-limit** command for global protection are as follows:

unauth-src-new-session: 300000

tcp: 300000

udp: 300000

icmp: 100000

other-protocol: 100000

By default, the **session-limit** command is disabled in a network attack defense domain.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide This command is used to limit the creation rate of various sessions.

Global protection is enabled by default. It needs to be disabled when the firewall performance and capacity are tested.

Configuration Examples The following example limits the creation rate of all sessions that pass through the device but do not pass the source verification to be lower than 10,000 per second.

```
FS(config)# defend-zone global
FS(config-defend-zone)# session-limit unauth-src-new-session    10000
```

25.1.21 scan

Use this command to set an anti-scanning policy. Use the **no** form of this command to cancel the anti-scanning policy. Use the **default** form of this command to restore the default settings.

scan { **in | out** } **src-ip threshold** { **low** | **medium** | **high** } [**timeout** *seconds*] **action** { **blocking** | **notify** }

no scan { **in | out** } **src-ip**

default scan { **in | out** } **src-ip**

Parameter Description

Parameter	Description
in	Detects the traffic that enters a network attack defense domain.
out	Detects the traffic that leaves a network attack defense domain.
low	Conducts detection at low sensitivity.
medium	Conducts detection at medium sensitivity.
high	Conducts detection at high sensitivity.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
notify	Records attacks only.
blocking	Blocks all traffic of an attack after the attack is identified.

Defaults No such a policy is configured by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide This command is used to defend against scanning behavior towards and from a network attack defense domain.

If the network segment, to which a protected interface belongs, is large (for example, the subnet mask is about 16 bits), you need to configure an anti-scanning policy in the network attack defense domain in routing mode. The purpose is to prevent switch abnormalities caused by scanning attacks.

Configuration Examples The following example configures an anti-scanning policy for detecting, at low sensitivity, scanning behavior from an external network towards the network attack defense domain named web. In the policy, when scanning behavior of a host is detected, all traffic of the host that enters or leaves the domain is blocked for 1,800 seconds.

```
FS(config)# defend-zone web
FS(config-defend-zone)# scan in src-ip threshold low timeout 1800 action blocking
FS(config-defend-zone)# exit
```

25.1.22 scan policy

Use this command to redefine default anti-scanning parameters. Use the **no** form of this command to delete defined default anti-scanning parameters. Use the **default** form of this command to restore the default settings.

scan policy

no scan policy

default scan policy

Parameter Description

Parameter	Description
N/A	N/A

Defaults You can run the **show scan parameter** command to display default values of parameters and current parameter configuration. For field descriptions, see the **show scan parameter** command.

Command Mode Global configuration mode

Default Level 14

Usage Guide This command is used to display the anti-scanning parameter configuration screen. It allows you to redefine default anti-scanning parameters for an anti-scanning policy.

Configuration Examples The following example displays the anti-scanning configuration screen.

```
FS(config)# scan policy
FS(config-scan-policy)# exit
```

Verification Run the **show scan parameter** command to display adjusted parameter results.

25.1.23 show defend

Use this command to display overall statistics on packet loss caused by NETWORK_DEFEND.

show defend drop

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to display overall statistics on packet loss caused by attack defense.

Configuration Examples The following example displays statistics on packet loss caused by attack defense.

```
FS# show defend drop
     Drops packet:          1,192
          Winnuke:          20
          Land:             80
          Global protect:   102
          Zone 'web':       890
          Zone 'ftp':       100
     Drops flow:              120
          Global protect:   50
      Zone 'web':           270
```

Field description:

Field	**Description**
Drops packet	Number of discarded packets
Drops flow	Number of discarded flows
Winnuke	Number of WinNuke attacks that are defended against
LAND	Number of LAND attacks that are defended against
Global protect	Number of attacks that are defended against by global protection
Zone	Network attack defense domain

Prompt Message If no packet is discarded in the defense against a type of attack, the attack item is not displayed.

25.1.24 show defend module

Use this command to display the overall work status of the current attack defense service module.

show defend module

Parameter Description

Parameter	**Description**

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to display the connection status of the current attack defense service module.

Configuration Examples

The following example displays the connection status of the current attack defense service module.

```
FS# show defend module
        Defend services module: 2
        Group       Slot       CPU         State
----------------------------------------
          0            3            0          Connect
          0            5            1          Online
```

Field description:

Field	Description
Defend services module	Number of connected attack defense service modules
Group	Attack defense service group
Slot	Slot of the service module
CPU	CPU number of the service module
State	Current status of the service module
Connect	Connection completed but service configuration uncompleted
Online	Connection completed and service configuration completed

25.1.25 show defend-zone

Use this command to display the status and statistics of a network attack defense domain.

show defend-zone *net-defend-zone-name* [**counters \| host**]

Use this command to display statistics of global protection.

show defend-zone global counters

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.
global	Indicates global protection.
counters	Indicates various statistics.
host	Displays the host statistics.

Command

Privileged EXEC mode

Mode

Default Level 14

Usage Guide This command is used to display the status, statistics, and attack information of a network attack defense domain.

Configuration Examples The following example displays the status of a network attack defense domain.

```
FS# show defend-zone web
        Description : web-servers-protect-zone
        Zone state: Running
        ACL associated: server-zone
        Traffic monitor: tcp, http, udp, icmp, ip
```

Field description:

Field	Description
Description	Description of the domain
Zone state	Status of the domain Running: The domain is running. Stopped: The domain is stopped. Learning: The domain is conducting learning.
ACL associated	Name of the associated ACL
Traffic monitor	Enabled traffic monitoring

The following example displays statistics of the network attack defense domain.

```
FS# show defend-zone web counters
        Counters :
                Received:               8234
                Forwarded:               7981
                Dropped(packets):       20
                Dropped(flows):         10
                Replied:                 105
        Dropped:
                Black-list:          0
                rate-limit:           5
                policy-drop(packets):15
                policy-drop(flows): 5
```

Field description:

Field	Description
Received	Number of packets received and processed by the domain
Forwarded	Number of forwarded packets
Dropped(packets)	Number of discarded packets
Dropped(flows)	Number of discarded flows
Replied	Number of response packets. The response packets are used for TCP SYN cookie.
Dropped	List of dropped packets

Black-list	Number of packets discarded due to the blacklist
rate-limit	Number of packets discarded due to the rate limit policy
policy-drop(packets)	Number of packets discarded due to other policies
policy-drop(flows)	Number of flows discarded due to other policies

The following example displays statistics of host objects relevant to the domain.

```
FS# show defend-zone web host
        Host protected (inside defend object): 178
        Host monitored (outside defend object): 5732
        Free host objects: 8372783 (Total)
```

Field description:

Field	Description
Host protected (inside defend object)	Number of monitored hosts in the network attack defense domain
Host monitored (outside defend object)	Number of monitored hosts outside the network attack defense domain
Free host objects	Number of idle host objects

25.1.26 show defend-zone traffic-snapshot

Use this command to display the current traffic snapshot of a network attack defense domain.

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**] }

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.
tcp	Indicates statistics on TCP data flows.
http	Indicates statistics on HTTP data flows.
ip	Indicates statistics on IP data flows.
udp	Indicates statistics on UDP data flows.
icmp	Indicates statistics on ICMP data flows.
syns-in	Indicates the rate of TCP SYN packets that enter the network attack defense domain.
conn-in	Indicates the number of concurrent connections that enter the network attack defense domain.
half-conn-in	Indicates the number of semi-connections that enter the network attack defense domain.
bandwidth	Indicates the bandwidth of traffic that enters the network attack defense domain.
topn	Lists the Top10 hosts.
pkts	Indicates the number of packets per second.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to display the current traffic snapshot of a network attack defense domain. You can define parameters so that the snapshot of a specific type of traffic is displayed.

Configuration Examples The following example displays a snapshot of all traffic.

```
FS# show defend-zone web traffic-snapshot
                      Total Pkts    current bps
  Received      1234567891       12567893
  Dropped              1934823             289302
  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
```

Field description:

Field	Description

Total Pkts	Number of packets
current bps	Current baud rate
Received	Statistics on received packets
Dropped	Statistics on discarded packets
Replied	Statistics on response packets
Syns in	Rate of SYN packets that enter the network attack defense domain
Connections(in)	Number of concurrent connections that enter the network attack defense domain
Half-connections (in)	Number of semi-connections that enter the network attack defense domain
Bandwidth (in)	Bandwidth of traffic that enters the network attack defense domain
Bandwidth (out)	Bandwidth of traffic that leaves the network attack defense domain
Pkts (in)	Number of packets that enter the network attack defense domain
Pkts (out)	Number of packets that leave the network attack defense domain

The following example displays a snapshot of current TCP connection creation rate and TopN hosts with the maximum rate.

```
FS #show defend-zone web traffic-snapshot tcp syns-in topN
    TCP FLOW
    Syns-in : 1200 pps
    Top 10 Sources:
          10.23.45.21         450
          121.2.65.90         350
          121.2.65.94         300
          121.2.62.97         120
          121.2.66.121        60
          121.2.61.9          35
          121.2.60.81         35
          121.2.60.82         23
          121.2.60.84         10
          121.2.60.86         8
```

Field description:

Field	Description
Top 10 Sources	Top 10 hosts that create the most connections

25.1.27 show defend-zone running-protect

Use this command to display ongoing attacks and protection in a network attack defense domain.

show defend-zone *net-defend-zone-name* **running-protect** [**tcp-auth** | **tcp-unauth** | **icmp** | **udp** | **other-protocol** | **scan** | *protect-id* | **attack** { **tcp-syn-flood** | **tcp-conn-flood** | **udp-spoof-flood** | **icmp-spoof-flood** | **other-spoof-flood** | **udp-flood** | **icmp-flood** | **other-flood** | **scan** }]

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.
tcp-auth	Indicates attacks that are defended against by a policy of the **tcp-auth** type.
tcp-unauth	Indicates attacks that are defended against by a policy of the **tcp-unauth** type.
icmp	Indicates attacks that are defended against by a policy of the **icmp** type.
udp	Indicates attacks that are defended against by a policy of the **udp** type.
other-protocol	Indicates attacks that are defended against by a policy of the **other-protocol** type.
protect-id	Indicates the protection policy ID. This ID uniquely identifies a protection policy that the system enables against each attack.
tcp-syn-flood	Indicates the TCP SYN flood attack type.
tcp-conn-flood	Indicates the TCP connection flood attack type.
udp-spoof-flood	Indicates the UDP flood attack type.
icmp-spoof-flood	Indicates the ICMP flood attack type.
other-spoof-flood	Indicates other flood attack type.
udp-flood	Indicates the UDP flood attack type.
icmp-flood	Indicates the ICMP flood attack type.
other-flood	Indicates other flood attack type.
scan	Indicates the scanning attack type.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to display ongoing attacks and protection in a network attack defense domain. The results can be displayed by attack defense policy or attack type.

Configuration Examples

The following example displays ongoing protection in the network attack defense domain.

```
FS # show defend-zone web running-protect
        Defend zone: 'web', Total report: 1
        Attack type: 'TCP SYN Flood'
  id: 823
             Begin:2012-5-9 12:03:04 ,timeout 60s
             Flow: * →    172.15.0.12, Action: Anti-spoofing(syn cookie)
             Policy: tcp-unauth:half-conn:dst_ip
             Threshold:100, current: 80
        Received:2300, Replied: 1300, Dropped:103, Auth host: 108
```

Field description:

Field	**Description**
Attack type	Attack type
id	Attack ID. A unique ID is generated for each attack instance.
Begin	Start time of an attack
timeout	Protection duration after an attack is stopped
Flow	Attack data flow. An asterisk (*) indicates that the IP address is not static.
Action	Protection behavior against the attack
Policy	Policy that identifies the attack
Threshold	Threshold
Received	Number of packets processed due to the protection policy
Replied	Number of response packets given due to the protection policy
Dropped	Number of packets discarded due to the protection policy
Auth host	Number of authenticated hosts

25.1.28 show defend-zone report

Use this command to display stopped attacks in a network attack defense domain.

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** }]

Parameter Description

Parameter	**Description**
net-defend-zone-name	Indicates the name of a network attack defense domain.
begin-date	Indicates the start date, in the format of YYYY-MM-DD.
begin-hour	Indicates the start hour. The value ranges from 0 to 23.
end-date	Indicates the end date, in the format of YYYY-MM-DD.
end-hour	Indicates the end hour. The value ranges from 0 to 23.
tcp-auth	Indicates attacks that are defended against by a policy of the **tcp-auth** type.
tcp-unauth	Indicates attacks that are defended against by a policy of the **tcp-unauth** type.
icmp	Indicates attacks that are defended against by a policy of the **icmp** type.
udp	Indicates attacks that are defended against by a policy of the **udp** type.
other-protocol	Indicates attacks that are defended against by a policy of the **other-protocol** type.
tcp-syn-flood	Indicates the TCP SYN flood attack type.
tcp-conn-flood	Indicates the TCP connection flood attack type.

udp-spoof-flood	Indicates the UDP flood attack type.
icmp-spoof-flood	Indicates the ICMP flood attack type.
other-spoof-flood	Indicates other flood attack type.
udp-flood	Indicates the UDP flood attack type.
icmp-flood	Indicates the ICMP flood attack type.
other-flood	Indicates other flood attack type.
scan	Indicates the scanning attack type.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to display stopped attacks in a network attack defense domain. The results can be displayed by attack defense policy or attack type. You can specify the date range.

✓ The network attack defense records attack reports of recent seven days.

Configuration Examples

The following example displays attack protection reports archived on 2012-5-9.

```
FS # show defend-zone web report 2012-5-9
    Defend zone: web, Total report: 1
   Attack type:    'TCP SYN Flood'
        2012-5-9 12:03:04 ~ 2012-5-9 15:06:04
        Flow: * -> 172.15.0.12, Action: Anti-spoofing(syn cookie)
        Policy: tcp-unauth:half-conn:dst_ip
        Threshold: 100, Action:    Anti-spoofing(syn cookie)
        Received: 10928, Replied: 8790, Dropped: 405
```

Field description:

Field	Description
2012-5-9 12:03:04 ~ 2012-5-9 15:06:04	Indicates the start time and end time of the attack.
Attack type	Attack type
Flow	Attack data flow. An asterisk (*) indicates that the IP address is not static.
Action	Protection behavior against the attack
Policy	Policy that identifies the attack
Threshold	Threshold
Received	Number of packets processed due to the protection policy
Replied	Number of response packets given due to the protection policy
Dropped	Number of packets discarded due to the protection policy

25.1.29 show net-defend learning

Use this command to display policy learning results of a network attack defense domain.

show net-defend learning *net-defend-zone-name*

Use the **global** form of this command to display policy learning results of global protection.

show net-defend learningglobal

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.
global	Indicates global protection.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to display policy learning results. You need to check a learned policy and adjust thresholds before configuring the policy on devices. Before the learning of a policy is over, you can also view the policy learning result, which is only traffic exporting policy for the current learning period.

Configuration Examples The following example displays policy learning results of a network attack defense domain.

```
FS# show net-defend learning web
Learning status: Finished (End time: 2012-3-12 15:00:30)
<TCP flow statistic (in)>
    Every dst-ip:
        Max half connection: 200
        Max syns (pps): 100
    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 dst-ip:
        Max UDP flow rate(pps): 3024
   Every auth-src-ip:
        Max UDP flow rate(pps): 1000
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 dst-ip threshold    200 action anti-spoofing
tcp-unauth half-conn-in global threshold    293829 action anti-spoofing
tcp-unauth syns-in dst-ip threshold    100 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
udp pkt-in dst-ip threshold 3024 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
```

Field description:

Field	Description
Learning status	Policy learning status
End time	End time
Every dst-ip	Every destination host
Every auth-src-ip	Every host that passes source verification (using an authentic IP address rather than a fake IP address)
Global	Entire domain
Max half connection	Maximum number of concurrent semi-connections
Max syns (pps)	Maximum rate of TCP SYN packets (pps)
Max connection	Maximum number of concurrent connections
Unauth-src UDP flow rate(pps)	Rate of UDP traffic that does not pass source verification (may be from fake source addresses)
Unauth-src ICMP flow rate(pps)	Rate of ICMP traffic that does not pass source verification (may be from fake source addresses)

Unauth-src Other-protocol flow rate(pps)	Rate of other types of traffic that does not pass source verification (may be from fake source addresses)
Max UDP flow rate(pps)	Maximum UDP packet rate
Max ICMP flow rate(pps)	Maximum ICMP packet rate
Max Other-protocol flow rate(pps)	Maximum rate of other type of packets

25.1.30 show scan parameter

Use this command to display anti-scanning parameter configuration.

show scan parameter

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to display anti-scanning parameter configuration. For modified parameters, the original default values are displayed in parentheses following the current values.

You can run the **scan policy** command to adjust default parameter values.

Configuration Examples The following example displays current anti-scanning parameters.

```
FS# show scan parameter
           Period         TimesNew conns      Rejected conns   IP count     port count
------------------------------------------------------------------------------------------
TCP(L)          100(60)        3(1)        NA             50                  30              30
TCP(M)          90             1           50             25                  25              25
TCP(H)          300            1           50             20                  20              20
UDP(L)          100(60)        3(1)        NA             50                  30              30
UDP(M)          90             1           50             20                  25              25
UDP(L)          300            1           50             17                  20              20
ICMP(L)         100(60)        3(1)        NA             50                  35              NA
ICMP(M)         90             1           40             25                  25              NA
ICMP(H)         300            1           30             20                  20              NA
Other-
protocol(L)  100(60)      3(1)        NA             50                  30              30
Other-
protocol(M)90             1           40             30                  25              25
Other-
protocol(H) 300           1           40             20                  20              20
```

Field description:

Field	**Description**

Period	Recovery period of the scanning behavior detection counter. If the number of scans detected in this period reaches the configured anti-scanning threshold, it is judged that a scanning attack occurs.
Times	Number of periods when a scanning behavior is detected. It is judged that a scanning attack occurs only after scans are detected in this number of consecutive periods.
New conns	Number of new abnormal connections, that is, number of new connections that do not enter the established state in the detection period.
Rejected cons	Number of connections rejected in the detection period, for example, connections for which the peer responds with RST or unreachable.
IP count	Number of changes on destination IP addresses of new connections in the detection period
Port count	Number of changes on destination ports of new connections in the detection period

25.1.31 stop net-defend learning

Use this command to stop policy learning in a network attack defense domain.

stop net-defend learning *net-defend-zone-name*

Use the **global** form of this command to stop policy learning of global protection.

stop net-defend learning global

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.
global	Indicates global protection.

Command Mode

Privileged EXEC mode

Default Level

14

Usage Guide

This command is used to stop policy learning.

Configuration Examples

The following example stops policy learning.

```
FS# stop net-defend learning web
```

25.1.32 sync defend config

Use this command to manually synchronize the current attack defense configuration to the kernel module.

sync defend config [*net-defend-zone-name*] [**force**]

Parameter Description

Parameter	Description
net-defend-zone-name	Indicates the name of a network attack defense domain.

force	Forcibly clears the attack defense configuration on the service module of the firewall and synchronizes configuration.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide When the attack defense module on the service module of the firewall malfunctions (for example, due to insufficient resources), you can synchronize the configuration to restore the status of the attack defense service module. This command is used to synchronize the current attack defense configuration.

If the name of a network attack defense domain is specified, this command synchronizes the configuration of this domain to the kernel service module of the firewall. If no domain name is specified, this command synchronizes all network attack defense configuration to the kernel service module of the firewall.

When the **force** keyword is used, the configuration on the service module of the firewall is cleared, and then the synchronization is started.

Configuration Examples The following example forcibly synchronizes all network attack defense configuration to the kernel service module of the firewall.

```
FS# sync defend config force
```

25.1.33 tcp

This command is used to configure global protection to defend all firewall traffic against TCP SYN Flood attacks. Use the **no** form of this command to cancel configuring global protection to defend all firewall traffic against TCP SYN Flood attacks. Use the **default** form of this command to restore the default settings.

tcp { **syns-in** | **half-conn-in** } **global threshold** *threshold-num* **action anti-spoofing**

no tcp { **syns-in** | **half-conn-in** } **global**

default tcp { **syns-in** | **half-conn-in** } **global**

Parameter Description

Parameter	**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.
threshold *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.
anti-spoofing	Conducts TCP SYN cookie anti-spoofing on traffic exceeding the threshold.

Defaults The default value of **syn-in** is 300,000 and the default value of **half-conn-in** is 4,000,000.

Command config-defend-zone configuration mode

Mode

Default Level 14

Usage Guide

This command is used to configure global protection to defend all firewall traffic against TCP SYN Flood attacks.

Attack defense is started when the rate of SYN packets that pass through the firewall exceeds the threshold or the number of TCP semi-connections exceeds the threshold.

Global protection is enabled by default. It needs to be disabled when the firewall performance and capacity are tested.

✓ No log is generated for global protection.

Configuration Examples

The following example conducts TCP SYN cookie anti-spoofing on the current device's TCP semi-connections out of 100,000.

```
FS(config)# defend-zone global
FS(config-defend-global)# tcp half-conn-in global    threshold 100000 action anti-spoofing
```

25.1.34 tcp-auth

Use this command to configure a policy for defending against TCP traffic from authentic source IP addresses. Use the **no** form of this command to cancel the policy for defending against TCP traffic from authentic source IP addresses. Use the **default** form of this command to restore the default settings.

tcp-auth { **conn-in** | **half-conn-in** | **syns-in** } **src-ip threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit** | **blocking** | **notify** }

no tcp-auth { **conn-in** | **half-conn-in** | **syns-in** } **src-ip**

default tcp-auth { **conn-in** | **half-conn-in** | **syns-in** } **src-ip**

Parameter Description

Parameter	Description
conn-in	Indicates the number of TCP connections initiated to a network attack defense domain.
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.
threshold *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.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
src-ip	Indicates that the policy is applied to identify packets from each source host.
limit	Limits the traffic below the value of *threshold-num*.
blocking	Blocks the traffic of the host that enters and leaves the attack defense domain.
notify	Records the attack event only.

Defaults

No such a policy is configured by default.

Command Mode

config-defend-zone configuration mode

Default Level

14

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 a network attack defense domain exceeds the threshold, the number of incomplete TCP handshake semi-connections (half-conn-in) exceeds the threshold, or the rate of initiated TCP SYN packets exceeds the threshold. The device limits the number of concurrent connections or the rate (according to the threshold) or blocks all traffic of the source host that enters or leaves the network attack defense domain (according to the policy execution time). The policy execution duration is not shorter than the value of *seconds*.

Configuration Examples

The following example configures a policy, in which when the number of TCP semi-connections initiated from a source host (using an authentic source IP address) to the network attack defense domain named web exceeds 200, the device is required to block all traffic of the host that enters or leaves the domain for 60s.

```
FS(config)# defend-zone web
FS(config-defend-zone)# tcp-auth half-conn-in src-ip threshold 200 timeout 3600 action blocking
FS(config-defend-zone)# exit
```

25.1.35 tcp-unauth

Use this command to enable a policy for defending against TCP SYN Flood attacks. Use the **no** form of this command to cancel the policy for defending against TCP SYN Flood attacks. Use the **default** form of this command to restore the default settings.

tcp-unauth { **syns-in** | **half-conn-in** } { **dst-ip** | **global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **anti-spoofing** | **notify** }

no tcp-unauth {**syns-in** | **half-conn-in** } {**dst-ip** | **global** }

default tcp-unauth {**syns-in** | **half-conn-in** } {**dst-ip** | **global** }

Parameter Description

Parameter	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.
threshold *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.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
dst-ip	Indicates that the policy is applied to identify packets sent to each destination host.
global	Indicates that the policy is applied to identify all packets that enter the domain.

anti-spoofing	Conducts TCP SYN cookie anti-spoofing on TCP SYN packets.
notify	Records the attack event only.

Defaults

No such policy is configured by default.

Command Mode

config-defend-zone configuration mode

Default Level

14

Usage Guide

The defense mechanism is enabled when the rate of SYN packets (syns-in) that enter a network attack defense domain exceeds the threshold or 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, and the execution time is not less 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 a network attack defense domain exceeds the threshold or the number of incomplete TCP handshake connections of the destination host exceeds the threshold. That is, the anti-forgery technology (anti-spoofing) is applied to all SYN packets destined for the host and the execution time is not less than the value of *seconds*.

Configuration Examples

The following example configures a policy, in which when the number of TCP semi-connections of any destination host in the network attack defense domain exceeds 1000, the device enables anti-spoofing on all TCP packets of the destination host.

```
FS(config)# defend-zone web
FS(config-defend-zone)# tcp-unauth half-conn-in dst-ip threshold 1000 action anti-spoofing
FS(config-defend-zone)# exit
```

25.1.36 threshold

Use this command to configure scanning detection thresholds for each sensitivity. Use the **no** form of this command to delete configured scanning detection thresholds of each sensitivity. Use the **default** form of this command to restore the default settings.

threshold { **low | medium | high** } **[protocol { tcp | udp | icmp | other-protocol }] { ip-count | port-count | new-conn | reject-conn }** *threshold-num*

no threshold { **low | medium | high** } **[protocol { tcp | udp | icmp | other-protocol }] { ip-count | port-count | new-conn | reject-conn }**

default threshold { **low | medium | high** } **[protocol { tcp | udp | icmp | other-protocol }] { ip-count | port-count | new-conn | reject-conn }**

Parameter Description

Parameter	Description
low	Indicates detection at low sensitivity.
medium	Indicates detection at medium sensitivity.
high	Indicates detection at high sensitivity.
icmp	Indicates the ICMP protocol.
other-protocol	Indicates protocols other than TCP, UDP, and ICMP.

tcp	Indicates the TCP protocol.
udp	Indicates the UDP protocol.
ip-count	Indicates the threshold of IP address changes in a scanning attack event.
port-count	Indicates the threshold of port changes in a scanning attack event.
new-conn	Indicates the threshold of new connections in a scanning attack event.
reject-conn	Indicates the threshold of rejected connections in a scanning attack event.
threshold-num	Indicates the threshold of scanning detection parameters. When the parameters are **ip-count**, **port-count**, and **reject-conn**, the value ranges from 1 to 2,000. When the parameter is **new-conn**, the value ranges from 10 to 2,000.

Defaults

You can run the **show scan parameter** command to display default values of parameters and current parameter configuration. For field descriptions, see the **show scan parameter** command.

Command Mode

config-scan-policy configuration mode

Default Level

14

Usage Guide

This command is used to set the anti-scanning detection threshold for each sensitivity.

Configuration Examples

The following example configures low-sensitivity detection and sets the threshold of TCP port changes to 100.

```
FS(config)# scan policy
FS(config-scan-policy)# threshold low protocol tcp port-count 100
```

Verification

Run the **show scan parameter** command to display adjusted parameter results.

25.1.37 traffic-monitor

Use this command to enable monitoring of different types of traffic. Use the **no** form of this command to disable monitoring of different types of traffic. Use the **default** form of this command to restore the default settings.

traffic-monitor { **tcp** | **http** | **udp** | **icmp | ip | all** }

no traffic-monitor { **tcp** | **http** | **udp** | **icmp | ip | all** }

default traffic-monitor { **tcp** | **http** | **udp** | **icmp | ip | all** }

Parameter Description

Parameter	Description
tcp	Monitors TCP traffic that enters a network attack defense domain.
http	Monitors HTTP traffic that enters a network attack defense domain.
udp	Monitors UDP traffic that enters a network attack defense domain.
icmp	Monitors ICMP traffic that enters a network attack defense domain.
ip	Monitors IP traffic that enters a network attack defense domain.
all	Monitors all traffic above.

Defaults

Traffic monitoring is disabled by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide This command is used to enable monitoring of traffic, including TCP, HTTP, UDP, ICMP, and IP traffic. If the **all** keyword is used, monitoring is enabled for all traffic.

Configuration Examples The following example enables TCP traffic monitoring for the network attack defense domain named web.

```
FS(config)#defend-zone web
FS(config-defend-zone)# traffic-monitor tcp
```

Verification Run the **show defend-zone** *net-defend-zone-name* **traffic-snapshot** command to display information about different types of traffic.

25.1.38 udp auth-src-in

Use this command to configure a policy for defending against UDP traffic from authentic source hosts. Use the **no** form of this command to cancel the policy for defending against UDP traffic from authentic source hosts. Use the **default** form of this command to restore the default settings.

udp auth-src-in src-ip threshold *threshold-num* [**timeout** *seconds*] **action** { **limit | blocking | notify** }

No udp auth-src-in src-ip

default udp auth-src-in src-ip

Parameter Description

Parameter	Description
auth-src-in	Indicates packets that enter a network attack defense domain and are from authentic source hosts.
src-ip	Indicates that the policy is applied to identify packets from each source host.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
limit	Limits the traffic below the value of *threshold-num*.
blocking	Blocks the traffic of the host that enters and leaves the attack defense domain.
notify	Records the attack event only.

Defaults No such policy is configured by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide When the rate of UDP traffic that is from any authentic source host and enters a network attack defense domain exceeds the threshold, the device starts the defense mechanism. The device limits the rate (not exceeding the threshold) of UDP packets that are from the source host and enter the network attack defense domain, or blocks all traffic of the source host that enters or leaves the network attack defense domain (according to the policy execution time). The policy execution duration is not shorter than the value of *seconds*.

Configuration Examples

The following example configures a policy, in which when the UDP packets sent from any authentic source host to the network attack defense domain named web exceeds 100 pps, the device is required to block all packets sent from this source IP address to the domain for 60 seconds.

```
FS(config)# defend-zone web
FS(config-defend-zone)# udp auth-src-in src-ip threshold 100 action blocking FS(config-defend-zone)# exit
```

25.1.39 udp pkt-in

Use this command to limit the UDP traffic that enters a network attack defense domain. Use the **no** form of this command to cancel the limit on UDP traffic that enters a network attack defense domain. Use the **default** form of this command to restore the default settings.

udp pkt-in { **dst-ip | global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit | notify** }

no udp pkt-in { **dst-ip | global** }

default udp pkt-in { **dst-ip | global** }

Parameter Description

Parameter	Description
pkt-in	Indicates all types of packets that enter a network attack defense domain.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
dst-ip	Indicates that the policy is applied to identify packets sent to each destination host.
global	Indicates that the policy is applied to identify all packets that enter the domain.
limit	Limits the traffic below the value of *threshold-num*.
notify	Records the attack event only.

Defaults

No such limit is configured by default.

Command Mode

config-defend-zone configuration mode

Default Level

14

Usage Guide

When the rate of UDP traffic that enters a network attack defense domain exceeds the threshold, the device limits the rate of the traffic to be lower than or equal to the threshold. The policy execution duration is not shorter than the value of *seconds*.

When the rate of UDP traffic destined for any host in a 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*.

Configuration Examples

The following example limits the rate of UDP packets sent to a host in the network attack defense domain named web to be lower than the threshold when the rate of UDP packets received by the host exceeds 100 pps.

```
FS(config)# defend-zone web
FS(config-defend-zone)# udp pkt-in dst-ip threshold 100 action limit
FS(config-defend-zone)# exit
```

25.1.40 udp unauth-src-in

Use this command to configure a policy for defending against UDP traffic that does not pass authentic source verification. Use the **no** form of this command to cancel the policy for defending against UDP traffic that does not pass authentic source verification. Use the **default** form of this command to restore the default settings.

udp unauth-src-in { **dst-ip** | **global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit** | **drop | notify** }

no udp unauth-src-in { **dst-ip** | **global** }

default udp unauth-src-in { **dst-ip** | **global** }

Parameter Description

Parameter	Description
unauth-src-in	Indicates packets that enter a network attack defense domain but do not pass authentic source verification.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
dst-ip	Indicates that the policy is applied to identify packets sent to each destination host.
global	Indicates that the policy is applied to identify all packets that enter the domain.
limit	Limits the traffic below the value of *threshold-num*.
drop	Discards the traffic.
notify	Records the attack event only.

Defaults

No such a policy is configured by default.

Command Mode

config-defend-zone configuration mode

Default Level

14

Usage Guide

When the rate of UDP packets that enter a network attack defense domain but do not pass the authentic 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 or discards all such packets.

When the rate of UDP packets that are destined for any host in a network attack defense domain but do not pass the authentic 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.

Configuration Examples

The following example configures a policy, in which when the rate of UDP packets using suspicious fake source IP addresses that are sent to the network attack defense domain named web exceeds 100 pps, the device is required to limit the rate of such packets to be lower than or equal to the threshold, and the device should keep the protection effective for 1 hour after the attack is stopped.

```
FS(config)# defend-zone web
FS(config-defend-zone)# udp unauth-src-in global threshold 100 timeout 3600 action limit
FS(config-defend-zone)# exit
```

25.1.41 other-protocol auth-src-in

Use this command to configure a policy for defending against other protocol traffic (except TCP, UDP, and ICMP traffic) from authentic source hosts. Use the **no** form of this command to cancel the policy for defending against other protocol traffic (except TCP, UDP, and ICMP traffic) from authentic source hosts. Use the **default** form of this command to restore the default settings.

other-protocol auth-src-in src-ip threshold *threshold-num* [**timeout** *seconds*] **action** { **limit | blocking | notify** }

no other-protocol auth-src-in src-ip

default other-protocol auth-src-in src-ip

Parameter Description

Parameter	Description
auth-src-in	Indicates packets that enter a network attack defense domain and are from authentic source hosts.
src-ip	Indicates that the policy is applied to identify packets from each source host.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
limit	Limits the traffic below the value of *threshold-num*.
blocking	Blocks the traffic of the host that enters and leaves the attack defense domain.
notify	Records the attack event only.

Defaults

No such policy is configured by default.

Command Mode

config-defend-zone configuration mode

Default Level

14

Usage Guide

When the rate of other protocol traffic (except TCP, UDP, and ICMP traffic) that is from any authentic source host and enters a 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, or blocks all traffic of the source host that enters or leaves the network attack defense domain (according to the policy execution time). The policy execution duration is not shorter than the value of *seconds*.

Configuration Examples

The following example configures a policy, in which when other protocol traffic sent from any authentic source host to the network attack defense domain exceeds 100 pps, the device is required to block the source host to send or receive any packets to or from the domain.

```
FS(config)#defend-zone web
FS(config-defend-zone)# other-protocol auth-src-in src-ip threshold 100 action blocking
FS(config-defend-zone)# exit
```

25.1.42 other-protocol pkt-in

Use this command to limit other protocol traffic (except TCP, UDP, and ICMP traffic) that enters a network attack defense domain. Use the **no** form of this command to cancel the limit on other protocol traffic (except TCP, UDP, and ICMP traffic) that enters a network attack defense domain. Use the **default** form of this command to restore the default settings.

other-protocol pkt-in { **dst-ip | global** } **threshold** *threshold-num* [**timeout** *seconds*] **action limit**

no other-protocol pkt-in { **dst-ip | global** }

default other-protocol pkt-in { **dst-ip | global** }

Parameter Description

Parameter	Description
pkt-in	Indicates all types of packets that enter a network attack defense domain.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
dst-ip	Indicates that the policy is applied to identify packets sent to each destination host.
global	Indicates that the policy is applied to identify all packets that enter the domain.
limit	Limits the traffic below the value of *threshold-num*.
notify	Records the attack event only.

Defaults

No limit is configured by default.

Command Mode

config-defend-zone configuration mode

Default Level

14

Usage Guide

When the rate of other protocol traffic (except the TCP, UDP, and ICMP traffic) that enters a network attack defense domain exceeds the threshold, the device will limit the rate of the traffic to be lower than or equal to the threshold. The policy execution duration is not shorter than the value of *seconds*.

When the rate of other protocol traffic (except the TCP, UDP, and ICMP traffic) destined for any host in a network attack defense domain exceeds the threshold, the device will limit the rate of the 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*.

Configuration Examples

The following example limits the rate of other protocol packets sent to a host in the network attack defense domain named web to be lower than the threshold when the rate of other protocol packets received by the host exceeds 100 pps.

```
FS(config)# defend-zone web
FS(config-defend-zone)# other-protocol pkt-in dst-ip threshold 100 action limit
FS(config-defend-zone)# exit
```

25.1.43 other-protocol unauth-src-in

Use this command to configure a policy for defending against other protocol traffic (except TCP, UDP, and ICMP traffic) that does not pass authentic source verification. Use the **no** form of this command to cancel the policy for defending against other protocol traffic (except TCP, UDP, and ICMP traffic) that does not pass authentic source verification. Use the **default** form of this command to restore the default settings.

other-protocol unauth-src-in { **dst-ip** | **global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit** | **drop |** **notify** }

no other-protocol unauth-src-in { **dst-ip** | **global** }

default other-protocol unauth-src-in { **dst-ip** | **global** }

Parameter Description

Parameter	Description
unauth-src-in	Indicates packets that enter a network attack defense domain but do not pass authentic source verification.
threshold *threshold-num*	Indicates the maximum number of packets per second. The value ranges from 1 to 100,000,000.
timeout *seconds*	Indicates the minimum execution duration of the policy, in seconds. The default value is 60. The value ranges from 10 to 86,400.
dst-ip	Indicates that the policy is applied to identify packets sent to each destination host.
global	Indicates that the policy is applied to identify all packets that enter the domain.
limit	Limits the traffic below the value of *threshold-num*.
drop	Discards the traffic.
notify	Records the attack event only.

Defaults No such policy is configured by default.

Command Mode config-defend-zone configuration mode

Default Level 14

Usage Guide When the rate of other protocol packets (except the TCP, UDP, and ICMP packets) that enter a network attack defense domain but do not pass the authentic 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 or discards all such packets.

When the rate of other protocol packets (except the TCP, UDP, and ICMP packets) that are destined for any host in a network attack defense domain but do not pass the authentic 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.

Configuration Examples

The following example configures a policy, in which when the rate of other protocol packets using suspicious fake source IP addresses that are sent to the network attack defense domain named web exceeds 100 pps, the device is required to limit the rate of such packets to be lower than or equal to the threshold, and the device should keep the protection effective for 1 hour after the attack is stopped.

```
FS(config)# defend-zone web
FS(config-defend-zone)# other-protocol unauth-src-in global threshold 100 timeout 3600 action limit
FS(config-defend-zone)# exit
```

25.2 Security Zone Commands

25.2.1 description

Use this command to configure a description string for a security zone. Use the **no** form of this command to delete the description string of a security zone. Use the **default** form of this command to restore the default settings.

description *string*

no description

default description

Parameter Description

Parameter	Description
string	Indicates the description string of a security zone. The value is a string of 1–40 characters.

Defaults

No description string is configured for a security zone by default.

Command Mode

Security zone mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example sets the description string of a security zone to trust.

```
FS(config-vfw)#security-zone hello
FS(config-vfw-security-zone)#description trust
```

Verification

Run the **show security-zone** command to display the description string of the security zone.

25.2.2 inner-zone-access

Use this command to allow IP mutual access within a security zone when the access policy of the security zone is not matched. Use the **no** form of this command to reject IP mutual access within a security zone when the access policy of the security zone is not matched. Use the **default** form of this command to restore the default settings.

inner-zone-access

no inner-zone-access

default inner-zone-access

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, IP mutual access is not allowed within a security zone when the access policy of the security zone is not matched.

Command Mode Security zone mode

Default Level 14

Usage Guide 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.

Configuration Examples The following example allows IP mutual access within the security zone named abc of the virtual firewall vfw1 when the access policy of the security zone is not matched.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#security-zone abc
FS(config-vfw-security-zone)#inner-zone-access
FS(config-vfw-security-zone)#description trust
```

Verification Run the **show security-zone** command to check whether IP mutual access is allowed within the security zone when the access policy of the security zone is not matched.

25.2.3 interface

Use this command to add an interface to a security zone. Use the **no** form of this command to delete an interface from a security zone. Use the **default** form of this command to restore the default settings.

interface *interface-name*

no interface *interface-name*

default interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Indicates the interface name.

Defaults An interface added to a virtual firewall belongs to the default security zone when it is not added to a security zone.

Command Mode Security zone mode

Default Level 14

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 a virtual firewall in non-routing mode, only VLAN interfaces can be added to a security zone.
- ✓ On a virtual firewall in routing mode (route-mode-vfw), layer-3 physical interfaces, layer-3 APs, and SVIs can be added to security zones.

Configuration Examples The following example adds interface vlan2 to the security zone named hello.

```
FS(config-vfw)#security-zone hello
FS(config-vfw-security-zone)#interface vlan 2
```

Verification Run the **show security-zone** command to display the interfaces associated with the security zone.

25.2.4 loose-inner-zone-access

Use this command to globally allow IP mutual access within a security zone when the intra–security zone access policy is not matched. Use the **no** form of this command to globally reject IP mutual access within a security zone when the intra–security zone access policy is not matched. Use the **default** form of this command to restore the default settings.

loose-inner-zone-access

no loose-inner-zone-access

default loose-inner-zone-access

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults By default, mutual access is no allowed when the inter–security zone access policy is not matched.

Command Mode Virtual firewall configuration mode

Default Level 14

Usage Guide

The priority of this command is lower than that of the **inner-zone-access** command.

Configuration Examples

The following example allows IP mutual access within security zones of the virtual firewall vfw1 when the intra–security zone access policy is not matched.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#loose-inner-zone-access
```

Verification

Run the **show security-access-global** command to display the global access policy of the security zone.

25.2.5 loose-inter-zone-access

Use this command to globally allow mutual access between security zones with the same security zone priority when the inter–security zone access policy is not matched. Use the **no** form of this command to globally reject mutual access between security zones with the same security zone priority when the inter–security zone access policy is not matched. Use the **default** form of this command to restore the default settings.

loose-inter-zone-access

no loose-inter-zone-access

default loose-inter-zone-access

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, mutual access is not allowed between security zones with the same security zone priority when the inter–security zone access policy is not matched.

Command Mode

Virtual firewall configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example allows mutual access between security zones with the same security zone priority when the inter–security zone access policy is not matched on the virtual firewall vfw1.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#loose-inter-zone-access
```

Verification

Run the **show security-access-global** command to display the global access policy of the security zone.

25.2.6 security-access

Use this command to configure a policy for IPv4 packet access from one security zone to another when ACL-based security zone access policies are used for packet matching. The policy is effective unidirectionally. Use the **no** form of this command to delete the ACL-based policy for IPv4 packet access from one security zone to another. Use the

default form of this command to restore the default settings.

security-access [**sequence** *sequence-number*] **from** *zone-name* **to** *zone-nameaccess-list* [**inactive**] [**description** *string*]

no security-access { **sequence** *sequence-number* | **from** *zone-name* **to** *zone-name access-list* }

default security-access { **sequence** *sequence-number* | **from** *zone-name* **to** *zone-name access-list* }

Use this command to configure a policy for IPv4 packet access from one security zone to another when object-based security zone access policies are used for packet matching. The policy is effective unidirectionally. Use the **no** form of this command to delete the object-based policy for IPv4 packet access from one security zone to another. Use the **default** form of this command to restore the default settings.

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*]

no 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*] }

default 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*] }

Use this command to activate an IPv4 access policy for a security zone. Use the **no** form of this command to deactivate the IPv4 access policy of a security zone.

security-access sequence *sequence-number* **active**

no security-access sequence *sequence-number* [**active**]

Parameter Description

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.
active	Indicates that a rule is activated.

Defaults No security zone access policy is configured for IPv4 packets by default.

Command Mode Virtual firewall configuration mode

Default Level 14

Usage Guide The name of the source security zone can be the same as that of the destination security zone. If the two security zones share the same name, the rule is an intra–security zone access policy.

ACL-based access policies cannot coexist with object-based access policies and they are controlled by the **security-access-match-object** command. Object-based access policies take effect only on security zones that are divided by network interface.

Configuration Examples The following example configures a unidirectional access policy for IPv4 packet access from security zone aaa to security zone bbb on the virtual firewall vfw1 and references an ACL named hello in the policy.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#security-access from aaa to bbb hello
```

The following example configures a unidirectional access policy for IPv4 packet access from security zone aaa to security zone bbb on the virtual firewall vfw1 and references the address object and service object in the policy.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#security-access sequence 10 from aaa to bbb permit src-address-object TERM dest-address-object
Server service myweb
```

Verification Run the **show security-access-rule** command to display the IPv4 packet access policy of the security zone.

25.2.7 security-access-match-object

Use this command to configure object-based matching when security zone access policies are used for packet matching. Use the **no** form of this command to restore the ACL-based matching when security zone access policies are used for patch matching. Use the **default** form of this command to restore the ACL-based matching when security zone access policies are used for patch matching.

security-access-match-object

no security-access-match-object

default security-access-match-object

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, ACL-based matching is adopted when security zone access policies are used for patch matching.

Command Mode

Virtual firewall configuration mode

Default Level

14

Usage Guide

After the **security-access-match-object** command is configured, the ACL-based security zone access policy configured using the **security-access** *access-list* command will be deleted and the command will be hidden. Likewise, after the **no security-access-match-object** command is configured, the object-based security zone access policy configured using the **security-access** [**sequence** *sequence-number*] command will be deleted and the command will be hidden.

✓ This command takes effect only on security zones divided by network interface.

Configuration Examples

The following example configures object-based matching when security zone access policies are used for packet matching on the virtual firewall vfw1.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#security-access-match-object
```

25.2.8 security-access-step

Use this command to configure the default sequence number step for security zone access policies. Use the **no** form of this command to restore the default sequence number step for security zone access policies to 10. Use the **default** form of this command to restore the default sequence number step for security zone access policies to 10.

security-access-step *step-number*

no security-access-step

default security-access-step

Parameter Description

Parameter	Description
step-number	Indicates the default sequence number step for the **security-access** and **security-access-ipv6** commands. The value ranges from 1 to 2,147,483,647.

Defaults

The default value is 10.

Command Mode

Virtual firewall configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example sets the default sequence number step for security zone access policies to 20 on the virtual firewall vfw1.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#security-access-step 20
```

Verification Run the **show security-access-global** command to display the default sequence number step of security zone access policies.

25.2.9 security-deny-access-log

Use this command to configure log generation (SYSLOG) in the case of packet discarding due to violation of a security zone access policy. Use the **no** form of this command to configure not to generate logs in the case of packet discarding due to violation of a security zone access policy. Use the **default** form of this command to restore the default settings.

security-deny-access-log

no security-deny-access-log

default security-deny-access-log

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults By default, logs are not generated in the case of packet discarding due to violation of a security zone access policy.

Command Mode Virtual firewall configuration mode

Default Level 14

Usage Guide This command is generally used for fault diagnosis only. The forwarding performance of the device will deteriorate after this command is enabled.

✓ When packets are discarded due to violation of a security zone policy, a log will be generated immediately if this command is configured. In the current version, the device can send logs only to the log server, but not to the console or buffer.

Configuration Examples The following example configures log generation in the case of packet discarding due to violation of a security zone access policy on the virtual firewall vfw1.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#security-deny-access-log
```

Verification Run the **show security-access-global** command to check whether logs are generated when packets are discarded due to violation of a security zone access policy.

25.2.10 security-level

Use this command to configure the priority for a security zone. Use the **no** form of this command to delete the priority of a security zone. Use the **default** form of this command to restore the default settings.

security-level *level-num*

no security-level

default security-level

Parameter Description

Parameter	Description
level-num	Indicates the priority of a security zone. The value ranges from 1 to 100. A larger value indicates a higher priority.

Defaults By default, a security zone has no priority.

Command Mode Security zone mode

Default Level 14

Usage Guide By default, a security zone has no priority for comparison.

Configuration Examples The following example sets the priority of a security zone to the maximum value.

```
FS(config-vfw)# security-zone hello
FS(config-vfw-security-zone)#security-level 100
```

Verification Run the **show security-zone** command to display the priority of the security zone.

25.2.11 security-permit-access-log

Use this command to configure log generation (SYSLOG) in the case of connection release after packet traffic matches a security zone policy. Use the **no** form of this command to configure not to generate logs in the case of connection release after packet traffic matches a security zone policy. Use the **default** form of this command to restore the default settings.

security-permit-access-log
no security-permit-access-log
default security-permit-access-log

Parameter Description

Parameter	Description
N/A	N/A

Defaults Logs are not generated when packets match a security zone policy.

Command Mode Virtual firewall configuration mode

Default Level 14

Usage Guide This command is generally used for fault diagnosis only. The forwarding performance of the device will deteriorate after this command is enabled.

✓ When packets match a security zone policy, logs can be generated only after connection release if this command is configured. In the current version, the device can send logs only to the log server, but not to the console or buffer.

Configuration Examples

The following example configures log generation in the case of connection establishment and release after packet traffic matches a security zone policy on the virtual firewall vfw1.

```
FS(config)#firewall-config vfw1
FS(config-vfw)#security-permit-access-log
```

Verification

Run the **show security-access-global** command to check whether logs are generated when a security zone access policy is matched.

25.2.12 security-zone

Use this command to create a security zone or go to an existing security zone. Use the **no** form of this command to delete the security zone. Use the **default** form of this command to restore the default settings.

security-zone *zone-name*

no security-zone *zone-name*

default security-zone *zone-name*

Parameter Description

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.

Defaults

No security domain is created and only the default security zone exists by default.

Command Mode

Virtual firewall configuration mode

Default Level

14

Usage Guide

A default security zone exists on each virtual firewall by default. You can run the **security-zone default** command to enter the configuration mode of the security zone. The default security zone can be neither created nor deleted.

Configuration Examples

The following example creates a security zone named hello on the virtual firewall vfw1.

```
FS(config-vfw)#security-zone hello
FS(config-vfw-security-zone)#
```

Verification

Run the **show security-zone** command to display information about the security zone.

25.2.13 security-zone-base interface

Use this command to divide security zones by network interface. Use the **no** form of this command to divide security zones by IP address set. Use the **default** form of this command to restore the default settings.

security-zone-base interface

no security-zone-base interface

default security-zone-base interface

Parameter Description

Parameter	Description
N/A	N/A

Defaults Security zones are divided by network interface by default.

Command Mode Virtual firewall configuration mode

Default Level 14

Usage Guide

- When the security zone division method is changed, all existing security zones, security zone access policies, and the global access policy 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.

Configuration Examples The following example divides security zones by IP address set on the virtual firewall vfw1.

```
FS(config-vfw)#no security-zone-base interface
```

The following example divides security zones by network interface on the virtual firewall vfw1.

```
FS(config-vfw)#security-zone-base interface
```

Verification Run the **show security-access-global** command to display the security zone division method.

25.2.14 show security-access-global

Use this command to display the global security zone access policy of a virtual firewall.

show security-access-global *firewall-name*

Parameter Description

Parameter	Description
firewall-name	Indicates the name of a virtual firewall.

Command Mode Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level 14

Usage Guide The global access policy has a lower priority than an inter–security zone access policy (or intra–security zone access policy if two security zones have the same name). The global access policy takes effect only when no inter–security zone access policy is matched. 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, security zone division method, whether a security zone access policy is based on an ACL or object, whether logs need to be generated in the case of connection establishment and release after a security zone policy is matched, whether logs need to be generated in the case of packet discarding due to violation of a security zone access policy, whether the function of collecting statistics on the inter–security zone policy matching is enabled, and sequence number step for security zone access policy commands.

Configuration Examples The following example displays the global access policy of the virtual firewall vfw1.

```
FS#show security-access-global vfw1
security zone is base interface
security rule is base ACL
inner-zone access:on
inter-zone access between same level:on
permit access log:off
deny access log:off
access statistics:off
web-auth enable:off
access rule step:10
```

Field description:

Field	Description
security zone is base	Security zone division method
security rule is base	Whether the security zone access policy is based on an ACL or object
inner-zone access	Whether IP mutual access is allowed within a security zone when the access policy of the security zone is not matched
inter-zone access between same level	Whether IP mutual access is allowed between security zones with the same security level when no inter–security zone access policy is matched
permit access log	Whether logs need to be generated in the case of connection establishment/release after a security zone policy is matched
deny access log	Whether logs need to be generated in the case of packet discarding due to violation of a security zone access policy
access statistics	Whether the function of collecting statistics on inter–security zone policy matching is enabled
web-auth enable	Whether Web authentication is enabled
access rules step	Sequence number step for the **security-access** and **security-access-ipv6** commands

25.2.15 show security-access-rules

Use this command to display the IPv4 packet access policy of a security zone.

show security-access-rules { [**from** *zone-name1*] *firewall-name* **|** [**to** *zone-name2*] *firewall-name* | *firewall-name* }

Parameter Description

Parameter	Description
zone-name1	Indicates the name of security zone 1.
zone-name2	Indicates the name of security zone 2.
firewall-name	Indicates the name of a virtual firewall.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

N/A

Configuration Examples

The following example displays all IPv4 access policies of the virtual firewall vfw1.

```
FS#show security-access-rules vfw1
security-access 100 from trust to untrust 10
security-access 101 from dmz to trust 20
security-aceess 102 from dmz to default 30
```

The following example displays all IPv4 access policies, in which the source security zone is trust, on the virtual firewall vfw1.

```
FS#show security-access-rules trust vfw1
security-access 100 from trust to untrust 10
security-access 101 from trust    to dmz 20
```

The following example displays all IPv4 access policies, in which the destination security zone is trustB, on the virtual firewall vfw1.

```
FS#show security-access-rules to trustB vfw1
security-access 100 from trustA    to trustB 10
security-access 101 from dmz    to trustB 20
```

Field description:

Field	Description
100	IPv4 ACL
101	IPv4 ACL
102	IPv4 ACL
trust	Name of a security zone
untrust	Name of a security zone
dmz	Name of a security zone
default	Name of a security zone
trustA	Name of a security zone
trustB	Name of a security zone

10	Sequence number
20	Sequence number
30	Sequence number

25.2.16 show security-zone

Use this command to display the configuration of a single or all security zones.

show security-zone [*zone-name*] *firewall-name*

Parameter Description

Parameter	**Description**
zone-name	Indicates the name of a security zone. By default, the configuration of all security zones is displayed.
firewall-name	Indicates the name of a virtual firewall.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

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 Examples

The following example displays the configuration of the security zone named TERM on the virtual firewall vfw1.

```
FS#show security-zone TERM vfw1
security-zone:TERM
description:terminal_client_zone
level: 80
inner-zone access:on
ip access-group:10
```

The following example displays the configuration of all security zones on the virtual firewall vfw1.

```
FS#show security-zone vfw1
security-zone:TERM
description:terminal_client_zone
level: 80
inner-zone access:on
ip access-group:10

security-zone:default
description:terminal_client_zone
level: 90
inner-zone access:on
```

Field description:

Field	Description
security- zone	Name of a security zone
description	Description string of the security zone
level	Priority of the security zone
inner-zone access	Whether IP mutual access is allowed within a security zone when the access policy of the security zone is not matched
ip access-group	ACL associated with the security zone

25.2.17 show security-zone-match

Use this command to display the matching of a security zone policy based on IPv4 packet characteristics.

show security-zone-match *ip-protocol source-ip dst-ip* **from** *src-interface* **to** *dst-interface firewall-name*

Use this command to display the matching of a security zone policy based on IPv4 TCP or UDP packet characteristics.

show security-zone-match { **6** | **17** | **tcp** | **udp** } *source-ip dst-ip* [*src-port dst-port*] **from** *src-interface* **to** *dst-interface firewall-name*

Use this command to display the matching of a security zone policy based on IPv4 ICMP packet characteristics.

show security-zone-match { **1** | **icmp** } *source-ip dst-ip* [*type code*] **from** *src-interface* **to** *dst-interface firewall-name*

Parameter Description

Parameter	Description
ip-protocol	Indicates the IP protocol.
1	Indicates the ICMP protocol.
6	Indicates TCP packets.
17	Indicates UDP packets.
tcp	Indicates TCP packets.
udp	Indicates UDP packets.
source-ip	Indicates the source IP address.
dst-ip	Indicates the destination IP address.
src-port	Indicates the source port number. The default port number is 0.
dst-port	Indicates the destination port number. The default port number is 0.
type	Indicates the ICMP type. The default value is 8.
code	Indicates the ICMP code. The default value is 0.
src-interface	Indicates the source interface.
dst-interface	Indicates the destination interface.
firewall-name	Indicates the name of a virtual firewall.

Command Mode

Privileged EXEC mode, global configuration mode, and interface configuration mode

Default Level

14

Usage Guide

This command is generally used for configuration diagnosis.

Configuration Examples

The following example displays the matching of a security zone policy based on IPv4 packet characteristics.

```
FS#show security-zone-match udp 192.168.1.1 192.168.2.1 3456 80 from vlan 2 to vlan 3 vfw1
Allowed for permitted by inner zone accessing control
```

Field description:

Field	Description
Denied for a unpredictable error occurs	Packets are rejected due to an internal error of the firewall.
Denied for inner-zone access is forbidden	Packets are rejected because access within the security zone is forbidden.
Denied for inter-zone access with same level is forbidden	Packets are rejected because the priority of the source security zone is the same as that of the destination security zone.
Denied for the level of src_zone is less than dst_zone's	Packets are rejected because the priority of the source security zone is lower than that of the destination security zone.
Denied for hitting a security zone rule (deny)	Packets are rejected because they match the deny rule in the security zone access policy.
Denied for not match the security policy	Packets are rejected because no relevant security zone access policy is found.
Allowed for the destination ip is a broadcast ip or multicast ip	Packets are allowed to pass because their destination IP addresses are a broadcast or multicast IP address.
Allowed for the destination ip is to local	Packets are allowed to pass because their destination IP addresses are the IP address of the local device.
Allowed for the source ip is a local ip	Packets are allowed to pass because their source IP addresses are the IP address of the local device.
Allowed for hitting a security zone rule	Packets are allowed to pass because they match a security zone policy.
Allowed for permitted by inner zone accessing control	Packets are allowed to pass because mutual access is allowed in the security zone.
Allowed for the level of src_zone is greater than dst_zone’s	Packets are allowed to pass because the priority of the source security zone is higher than that of the destination security zone.
Allowed for the level of dst_zone is equal to src_zone’s	Packets are allowed to pass because the priority of the source security zone is the same as that of the destination security zone.

Chapter 12 WLAN QoS Configuration Commands

1 WLAN QoS Commands

1.1 ap-based

Use this command to configure the upstream and downstream traffic rate limit of the current AP.

Use the **no** form of this command to restore the default setting.

ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

no ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent total-user-limit of the current AP.

Use the **no** form of this command to restore the default setting.

ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**

no ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**

Parameter Description

Parameter	**Description**
per-user-limit	Limit for each user on the AP
total-user-limit	Limit for the entire AP
down-streams	Downstream traffic limit of the AP
up-streams	Upstream traffic limit of the AP
intelligent	Enables intelligent rate limit.
average-data-rate	Average rate limit, ranging from 8 to 261,120 in the unit of 8Kbps.
burst-data-rate	Burst rate limit, ranging from 8 to 261,120 in the unit of 8Kbps.

Defaults The traffic limit and intelligent total-user-limit are disabled by default.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the average downstream rate of the AP 1 to 800 Kbps and the burst rate to 1,600 Kbps.

```
FS(config)# ap-config wlan-ap-001
FS(config-ap)# ap-based down-streams average-data-rate 800 burst-data-rate 1600
```

Related Commands

Command	**Description**
netuser H.H.H { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the client-based in-band and out-of-band traffic rate limit.
wlan-based { **down-streams** | **up-streams** }	Configures the WLAN-based upstream and

average-data-rate *average-data-rate* **burst-data-rate** *burst-data-rate*	downstream traffic rate limit.

Platform Description

This command is supported on ACs.

1.2 fair-schedule

Use this command to enable fair scheduling on the wireless AP.

Use the **no** form of this command to disable this function.

fair-schedule

no fair-schedule

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command mode

AC: AP configuration mode

Fat AP: AP configuration mode

Usage Guide

- On a fat AP, the command of configuring fair scheduling is used in configuration mode and you can use the **show run** command to show configuration.
- When the AP works in fit AP mode, the fair scheduling can be configured only on the AC.

Configuration Examples

The following example disables fair scheduling on the AP.

```
FS(config)# ap-config ap-name
FS(wids-config)# no fair-schedule
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on ACs and fat APs.

1.3 illegal-sta-check

Use these commands to enable anti-proxy detection.

Use the **no** form of these commands to restore the default setting.

illegal-sta-check ip ttl

illegal-sta-check tcp source-ports [*port-num*]

no illegal-sta-check ip ttl

no illegal-sta-check tcp source-ports

Parameter Description

Parameter	**Description**
port-num	Sets the maximum number of detection ports, in the range from 1 to 512. The default is 512.

Defaults The anti-proxy detection is disabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Example The following example enables anti-proxy detection on ap1 with the TTL policy.

```
FS(config)# ap-config ap1
FS(config-ap)#illegal-sta-check ip ttl
```

The following example enables anti-proxy detection on ap2 with the source-port-detection policy. The default port number is 512.

```
FS(config)# ap-config ap2
FS(config-ap)#illegal-sta-check tcp source-ports
```

Platform Description This command is supported on ACs and fat APs.

1.4 netuser

Use this command to configure the in-band and out-of-band traffic limit for a specified user in the current WLAN.

Use the **no** form of this command to restore the default setting.

netuser *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

no netuser *mac-address* { **inbound** | **outbound** }

Parameter Description

Parameter	**Description**
mac-address	User's MAC address to be set.
inbound	User’s in-band traffic limit.
outbound	User’s out-of-band traffic limit.
average-data-rate	Average rate limit, ranging from 8 to 261,120 in the unit of 8Kbps.
burst-data-rate	Burst rate limit, ranging from 8 to 261,120 in the unit of 8Kbps.

Defaults No traffic limit is set by default.

Command mode AC configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the average in-band rate to 800Kbps and burst rate to 1,600 Kbps for the user 0000.0000.0001 in WLAN 1.

```
FS(config)# wlan-config 1
FS(wids-config)# netuser 0000.0000.0001 inbound average-data-rate 800 burst-data-rate 1600
```

Related Commands

Command	Description
wlan-based { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the WLAN-based upstream and downstream traffic rate limit.
ap-based { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the AP-based in-band and out-of-band traffic rate limit.

Platform Description This command is supported on ACs.

1.5 show dot11 ratelimit

Use this command to display WLAN rate limit information.

show dot11 ratelimit { **wlan** | **ap** | **user** }

show dot11 ratelimit wlan perap

Parameter Description

Parameter	Description
wlan	Displays the rate limit information of all WLANs.
ap	Displays the rate limit information of all APs.
user	Displays the rate limit information of all users.
perap	Displays the total WLAN rate limit information of all APs.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the rate limit information of all APs.

```
FS# show dot11 ratelimit ap
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on ACs.

1.6 sta-fair

Use this command to specify the fair scheduling priority for a specified user.

Use the **no** form of this command to restore the default setting.

sta-fair *mac-address* **priority** *priority*

no sta-fair *mac-address*

Parameter Description

Parameter	Description
mac-address	Specifies the user's MAC address.
priority	Sets the fair scheduling priority, in the range from 1 to 6.

Defaults The default is 1 for all STAs by default.

Command Mode Fit AP: Global configuration mode

Fat AP: AC configuration mode

Usage Guide N/A

Configuration Example The following example sets the fair scheduling priority for user 0000.0000.0001 on the AC to 3.

```
FS(config)# ac-controller
FS(config-ac)# sta-fair 0000.0000.0001 priority 3
```

Platform Description This command is supported on ACs and fat APs.

1.7 wlan-based

Use this command to configure the upstream and downstream traffic limit of the current WLAN.

Use the **no** form of this command to restore the default setting.

wlan-based { **per-user-limit** | **total-user-limit** | **per-ap-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

no wlan-based { **per-user-limit** | **total-user-limit** | **per-ap-limit** } { **down-streams** | **up-streams }**

Use this command to configure the intelligent per-ap-limit of the current WLAN.

Use the **no** form of this command to restore the default setting.

wlan-based per-ap-limit { **down-streams** | **up-streams** } **intelligent**

no wlan-based per-ap-limit { **down-streams** | **up-streams** } **intelligent**

Parameter Description

Parameter	Description
per-user-limit	Limit for each user on the WLAN.
total-user-limit	Limit for the entire WLAN.
per-ap-limit	Limit WLAN Total for each AP.
down-streams	Total downstream traffic limit of the WLAN.
up-streams	Total upstream traffic limit of the WLAN.
intelligent	Whether to enable intelligent per-ap-limit.
average-data-rate	Average rate limit, ranging from 8 to 261120 in the unit of 8Kbps.
burst-data-rate	Burst rate limit, ranging from 8 to 261120 in the unit of 8Kbps.

Defaults

The function is disabled by default.

Command mode

WLAN configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the average downstream rate of WLAN 1 to 800 Kbps and burst rate to 1,600 Kbps.

```
FS(config)# wlan-config 1
FS(wids-config)# wlan-based down-streams average-data-rate 800 burst-data-rate 1600
```

Related Commands

Command	Description
ap-based { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the AP-based in-band and out-of-band traffic rate limit.
netuser *H.H.H* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the Client-based in-band and out-of-band traffic rate limit.

Platform Description

This command is supported on ACs.

1.8 wlan-qos ap-based

Use this command to configure the upstream and downstream traffic limit of the current AP.

Use the **no** form of this command to restore the default setting.

wlan-qos ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

no wlan-qos ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent total-user-limit for of the current AP.

Use the **no** form of this command to restore the default setting.

wlan-qos ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**

no wlan-qos ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**

Parameter Description

Parameter	Description
per-user-limit	Limit for each user on the AP.
total-user-limit	Limit for the entire AP.
down-streams	Total downstream traffic limit of the AP.
up-streams	Total upstream traffic limit of the AP.
intelligent	Whether to enable intelligent total-user-limit.
average-data-rate	Average rate limit, ranging from 8 to 261,120 in the unit of 8 Kbps.
burst-data-rate	Burst rate limit, ranging from 8 to 261,120 in the unit of 8 Kbps.

Defaults These functions are disabled by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the average downstream rate of AP wlan-ap-001 to 800 Kbps and burst rate to 1,600 Kbps.

```
FS(config)# wlan-qos ap-based per-user-limit down-streams average-data-rate 800 burst-data-rate 1600
```

Related Commands

Command	Description
wlan-qos netuser *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the Client-based in-band and out-of-band traffic rate limits.
wlan-qos wlan-based { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the WLAN-based in-band and out-of-band traffic rate limits.

Platform Description This command is supported on fat APs.

1.9 wlan-qos netuser

Use this command to configure the in-band and out-of-band traffic limits for a specified user in the current WLAN.

Use the **no** form of this command to restore the default setting.

wlan-qos netuser *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

no wlan-qos netuser *mac-address* { **inbound** | **outbound** }

Parameter Description

Parameter	Description
mac-address	User's MAC address to be set.
inbound	User’s in-band traffic limit.
outbound	User’s out-of-band traffic limit.
average-data-rate	Average rate limit, ranging from 8 to 261120 in the unit of 8Kbps.
burst-data-rate	Burst rate limit, ranging from 8 to 261120 in the unit of 8Kbps.

Defaults No traffic limit is set by default.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the average in-band rate to 800 Kbps and burst rate to 1,600 Kbps for the user 0000.0000.0001 in WLAN 1.

```
FS(config)# wlan-qos netuser 0000.0000.0001 inbound average-data-rate 800 burst-data-rate 1600
```

Related Commands

Command	Description
wlan-qos wlan-based { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit}** { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the WLAN-based in-band and out-of-band traffic rate limits.
wlan-qos ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the AP-based in-band and out-of-band traffic rate limits.

Platform Description This command is supported on fat APs.

1.10 wlan-qos wlan-based

Use this command to configure the upstream and downstream traffic limit of the current WLAN.

Use the **no** form of this command to restore the default setting.

wlan-qos wlan-based { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

no wlan-qos wlan-based { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent total-user-limit of the current WLAN. Use the **no** form of this command to restore the default setting.

wlan-qos wlan-based { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams** } **intelligent**

no wlan-qos wlan-based { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams }** **intelligent**

Parameter Description

Parameter	Description
wlan-id	WLAN ID.
ssid	SSID configured by the WLAN.
per-user-limit	Limit for each user on the WLAN.
total-user-limit	Limit for the entire WLAN.
down-streams	Total downstream traffic limit of the WLAN.
up-streams	Total upstream traffic limit of the WLAN.
intelligent	Whether to enable intelligent total-user-limit.
average-data-rate	Average rate limit, ranging from
burst-data-rate	Burst rate limit, ranging from 8 to 261120 in the unit of 8Kbps.

Defaults The traffic limit and intelligent total-user-limit are disabled by default.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example configures the average downstream rate of WLAN 1 to 800Kbps and burst rate to 1600Kbps.

```
FS(config)# wlan-based 1 per-user-limit down-streams average-data-rate 800 burst-data-rate 1600
```

Related Commands

Command	Description
wlan-qos ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the AP-based in-band and out-of-band traffic rate limits.
netuser *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*	Configures the Client-based in-band and out-of-band traffic rate limits.

Platform Description This command is supported on fat APs.

1.11 wqos fs enable

Use this command to enable WQoS traffic statistics.

Use the **no** form of this command to restore the default setting.

wqos fs enable

no wqos fs enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode

AP: Global configuration mode

AC: AC configuration mode

Usage Guide

When dot1x authentication and Web authentication are disabled, use this command to enable WQoS traffic statistics. Otherwise, WQoS traffic statistics is enabled by default and this command becomes invalid.

Configuration Example

The following example enables WQoS traffic statistics for all APs associated with the AC.

```
FS(config-ac)#wqos fs enable
```

Platform Description

This command is supported on APs.

1.12 wqos radio rate-guarantee

Use this command to enable rate-guarantee function for a specified radio.

Use the **no** form of this command to restore the default setting.

wqos radio *radio_id* **rate-guarantee enable**

no wqos radio *radio_id* **rate-guarantee enable**

Use this command to configure the overall bandwidth under a specific RF mode.

Use the **no** form of this command to restore the default setting.

wqos radio *radio_id* **rate-guarantee** { **802.11a** | **802.11b** | **802.11g** | **802.11n** | **802.11ac** } **bandwidth** *average-data-rate*

no wqos radio *radio_id* **rate-guarantee** { **802.11a** | **802.11b** | **802.11g** | **802.11n** | **802.11ac** } **bandwidth**

Use this command to configure the rate-guarantee bandwidth proportion for an associated WLAN.

wqos radio *radio_id* **rate-guarantee wlan** *wlan_id* **percent** *percent*

Parameter Description

Parameter	Description
radio_id	AP radio ID. The range is from 1 to 16.
802.11a	802.11a mode
802.11b	802.11b mode

802.11g	802.11g mode
802.11n	802.11n mode
802.11ac	802.11ac mode
average-data-rate	Specifies the overall bandwidth. The unit is Kbps. 802.11n: 2-31,250 802.11a: 2-3,750 802.11b: 2-875 802.11g: 2-3,750 802.11ac: 2-93,750
wlan_id	The WLAN associated with the specified radio Fit AP: 1-4,094 , Fat AP: 1-32
percent	The proportion of rate-guarantee bandwidth: 1-100

Defaults

By default, the rate-guarantee function is disabled, the WLAN rate-guarantee proportion is 0% and the overall bandwidth under different RF modes are as follows:

802.11n: 31,250

802.11a: 3,750

802.11b: 875

802.11g: 3,750

802.11ac: 93,750

Command Mode

Fit AP: AP group configuration mode

Fat AP: Global configuration mode

Usage Guide

- Only after the rate-guarantee function is enabled, the overall bandwidth and WLAN bandwidth proportion configurations will take effect. The actual bandwidth will be no more than the overall bandwidth.
- The total WLAN bandwidth proportion cannot be larger than 100%. For a specified radio, the absolute rate-guarantee bandwidth will be figured out based on the overall bandwidth and bandwidth proportion. Once in congestion, WLANs under the radio will get that bandwidth assurance.

Configuration Examples

The following example configures the overall bandwidth under 802.11 mode.

```
FS(config)# ap-group ap-group1
FS(config-group)# wqos radio 1 rate-guarantee 802.11n bandwidth 5000
```

The following example configures the rate-guarantee bandwidth proportion for WLAN 1.

```
FS(config)# ap-group ap-group1
FS(config-group)# wqos radio 1 rate-guarantee wlan 1 percent 50
```

The following example enables the rate-guarantee functions for radio 1.

```
FS(config)# ap-group ap-group1
FS(config-group)# wqos radio 1 rate-guarantee enable
```

Platform Description	N/A

2 WMM Commands

2.1 wlan-qos map-table

Use this command to configure packet priority mapping for the current WLAN. Use the **no** form of this command to restore the default setting.

wlan-qos map-table { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value* **export** *export-tag-value*

no wlan-qos map-table { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value*

Parameter Description

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. WMM (dot11e) is one of QoS fields of 802.11 wireless protocol headers. It refers to WLAN priority, in the range from 0 to 7. DSCP is the priority field of IP protocol headers, in the range from 0 to 63. The default is 0.
export *export-tag-value*	Sets priority of the outgoing packet. WMM (dot11e) is one of QoS fields of 802.11 wireless protocol headers. It refers to WLAN priority, in the range from 0 to 7. DSCP is the priority field of IP protocol headers, in the range from 0 to 63. The default is 0.

Defaults

DSCP-to-dot11e Mapping Table

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

dot11e-to-DSCP Mapping Table

802.11e	DSCP
0	0
3	8
1	16
2	24
4	32
5	40

6	48
7	56

Command Mode

WLAN configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

ⓘ The parameters **dot11e-tunnel-dscp**, **dot11e-inner-dscp**, and **dot11e-dscp** are not available on the fat AP.

Configuration Examples

The following example sets priority mapping from DSCP to dot11e. The priority of the incoming original packet is 1 and that of the outgoing packet is 10.

```
FS# configure terminal
FS(config)# wlan-config 1
FS(config-wlan)# wlan-qos map-table dscp-dot11e import 1 export 10
```

Platform Description

N/A

2.2 wmm dot1p enable

Use this command to enable 802.11p QoS mapping policy mechanism. Use the **no** form of this command to restore the default setting.

wmm dot1p enable radio *radio-id*

no wmm dot1p enable radio *radio-id*

Parameter Description

Parameter	Description
radio *radio-id*	Specifies the radio on which 802.11p QoS mapping policy mechanism is enabled/disabled, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports the configuration of this parameter.

Defaults

This function is disabled by default.

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

Configuration Examples

The following example enables 802.11p QoS mapping policy mechanism for radio 1 on VOICE-AP.

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm dot1p enable radio 1
```

Platform Description

N/A

2.3 wmm dot1p policy

Use this command to configure how to apply the 802.11p QoS mapping policy mechanism for the AP. Use the **no** form of this command to restore the default setting.

wmm dot1p policy 1q [*1q-policy-value*] **radio** *radio-id*

no wmm dot1p policy radio [*radio-id*]

Parameter Description

Parameter	Description
1q *1q-policy-value*	Applies the 802.11p QoS mapping policy mechanism, in the range from 0 to 1. The default is 0. Q=1: AP tags the priority domain of 802.1Q according to 802.1p. Q=0: AP tags the priority domain of 802.1Q according to the user priority in the **Qos Control** field of IEEE 802.11 headers. Apply "Q=1" method when there is no **QoS Control** field.
radio *radio-id*	Specifies the radio on which 802.11p QoS mapping policy mechanism is applied, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports the configuration of this parameter.

Defaults

The default is 0.

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

The configuration is valid only when the 802.11p QoS mechanism is enabled.

Configuration Examples

The following example tags the priority domain of 802.1Q for radio 1 on VOICE-AP.

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm dot1p 1q 1 radio 1
```

Platform Description

N/A

2.4 wmm dot1p tag

Use this command to configure 802.1p priority. Use the **no** form of this command to restore the default setting.

wmm dot1p tag [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

no wmm dot1p tag { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

Parameter Description

Parameter	Description
tag *tag-value*	Sets the 802.1p priority, in the range from 0 to 7.
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*	Specifies the radio on which 802.11p priority is configured, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.

Defaults

The default **best-effort** is 0; the default **back-ground** is 2; the default **video** is 4; the default **voice** is 6.

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

The configuration is valid only when the 802.11p QoS mechanism is enabled.

Configuration Examples

The following example sets 802.1p priority to 5 for radio 1 on VOICE-AP.

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm dot1p tag 5 voice radio 1
```

Platform Description

N/A

2.5 wmm dscp enable

Use this command to enable DSCP QoS mapping policy mechanism. Use the **no** form of this command to restore the default setting.

wmm dscp enable radio *radio-id*

no wmm dscp enable radio *radio-id*

Parameter Description

Parameter	Description
radio *radio-id*	Specifies the radio on which DSCP QoS mapping policy mechanism is enabled/disabled, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.

Defaults

This function is disabled by default.

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

Configuration Examples

The following example enables DSCP QoS mapping policy mechanism for radio 1 on VOICE-AP.

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm dscp enable radio 1
```

Platform Description

N/A

2.6 wmm dscp policy

Use this command to configure how to apply the DSCP QoS mapping policy mechanism for the AP. Use the **no** form of this command to restore the default setting.

wmm dscp policy outer-tunnel [*outer-tunnel-value*] **inner-tunnel** [*inner-tunnel-value*] **radio** *radio-id*

no wmm dscp policy radio *radio-id*

Parameter Description

Parameter	Description
outer-tunnel *outer-tunnel-value*	Configures how to apply the DSCP QoS mapping policy mechanism for the outer tunnel header, in the range from 0 to 1. The default is 0. In the centralized forwarding mode: O=1: AP sets DSCP domain for the tunnel header according to pushed configuration policy; O=0: AP sets DSCP domain for the tunnel header according to inner tunnel packets. If inner tunnel packets are encrypted or non-IPv4, the "O=1" method will be applied. In the local forwarding mode: O=1: invalid value; O=0: invalid value.
inner-tunnel *inner-tunnel-value*	Configures how to apply the DSCP QoS mapping policy mechanism for the inner tunnel header, in the range from 0 to1. The default is 0. In the centralized forwarding mode: AP sets DSCP domain for the tunnel header according to inner tunnel packets; If inner tunnel packets are encrypted or non-IPv4, the "I=1" method will be applied. I=0: AP cannot modify the DSCP domain of user packets. In the local forwarding mode: I=1: AP configures the DSCP domain for user packets according to the pushed

	configuration policy. I=0: AP cannot modify the DSCP domain of user packets.
radio *radio-id*	Specifies the radio on which DSCP QoS mapping policy mechanism is applied, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.

Defaults The default is 0.

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

The configuration is valid only when the DSCP QoS mechanism is enabled.

Configuration Examples

The following example sets both outer and inner tunnel headers to 0 for DSCP mapping mechanism of radio 1 on VOICE-AP.

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm dscp outer-tunnel 0 inner-tunnel 0 radio 1
```

Platform Description N/A

2.7 wmm dscp tag

Use this command to configure the DSCP identification. Use the **no** form of this command to restore the default setting.

wmm dscp tag [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

no wmm dscp tag { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

Parameter Description

Parameter	**Description**
tag *tag-value*	Sets the DSCP priority, in the range from 0 to 63.
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*	Specifies the radio on which the DSCP identification is configured, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.

Defaults The default **best-effort** is 0; the default **back-ground** is 16; the default **video** is 32; the default **voice** is 48.

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

DSCP identification is valid only when the DSCP mechanism is enabled.

Configuration Examples

The following example sets the DSCP identification to 5 for voice queue of radio 1 on VOICE-AP.

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm dscp tag 5 voice radio 1
```

Platform Description

N/A

2.8 wmm edca-client

Use this command to configure the EDCA parameters for the client. Use the **no** form of this command to restore the default setting.

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*

no wmm edca-client { **back-ground** | **best-effort** | **video** | **voice** } [**length**] **radio** *radio-id*

Parameter Description

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, in the range from 1 to15.
cwmin *cwmin-value*	Sets the **cwmin** value, in the range from 0 to 15.
cwmax *cwmax-value*	Sets the **cwmax** value, in the range from 0 to 15.
txop *txop-value*	Sets the **txop** value, in the range from 0 to 255 in the unit of 32 μs.
length *queue-length*	Sets the AC queue length in the range from 1 to 255. The default is 255.
radio *radio-id*	Specifies the radio on which the client EDCA parameters are configured, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.

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

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

⚠ The **cwmax** value must be greater than the **cwmin** value. Otherwise, a configuration error message is displayed.

Configuration Examples

The following example configures **asfsn** to 2, **cwmin** to 2, **cwmax** to 3 and **txop** to 50 for the voice queue of radio 1 on VOICE-AP.

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1
```

Platform Description

N/A

2.9 wmm edca-radio

Use this command to configure the EDCA parameters for the AP. Use the **no** form of this command to restore the default setting.

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*

no wmm edca-radio { **back-groud** | **best-effort** | **video** | **voice** } [**noack**] **radio** *radio-id*

Parameter Description

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, in the range from 1 to 15.
cwmin *cwmin-value*	Sets the **cwmin** value, in the range from 0 to 15.
cwmax *cwmax-value*	Sets the **cwmax** value, in the range from 0 to 15.
txop *txop-value*	Sets the **txop** value, in the range from 0 to 255 in the unit of 32 µs.
noack	Indicates that the no ack policy is enabled. The no ack policy is disabled by default.
radio *radio-id*	Specifies the radio on which the client EDCA parameters are configured, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.

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

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

The configuration takes effect after the WMM service is enabled.

ℹ According to the IEEE 802.11 standard, no ACK is returned for multicast or broadcast frames.

⚠ The **cwmax** value must be greater than the **cwmin** value. Otherwise, a configuration error message is displayed.

Configuration Examples

The following example sets **aifsn** to 1, **cwmin** to 1, **cwmax** to 3, **txop** to 50 for the voice queue of radio 1 on VOICE-AP.

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
```

Platform Description

N/A

2.10 wmm enable

Use this command to enable the WMM service. Use **no** form of this command to disable the WMM service.

wmm enable radio *radio-id*

no wmm enable radio *radio-id*

Parameter Description

Parameter	**Description**
radio *radio-id*	Specifies the radio on which the WMM service is enabled/disabled, in the range from 1 to 48. This parameter is not available on the fat AP. Only the AC supports configuration of this parameter.
no	Disables the WMM service.

Defaults

This function is enabled by default.

Command Mode

Fit AP: AP configuration mode

Fat AP: Interface configuration mode

Usage Guide

When the WMM service is disabled, the default priority queue is used for reception and mapping.

Configuration

The following example enables the WMM service for radio 1 on VOICE-AP.

Examples

```
FS# configure terminal
FS(config)# ap-config VOICE-AP
FS(config-ap)# wmm enable radio 1
```

Platform Description

N/A

Chapter 13 WLAN RF Configuration Commands

1. Band Select Commands

1 Band Select Commands

1.1 band-select acceptable-rssi

Use this command to configure an acceptable STA RSSI lower limit. Use the **no** form of this command to restore the default setting.

band-select acceptable-rssi *value*

no band-select acceptable-rssi

Parameter Description

Parameter	Description
value	Indicates acceptable STA RSSI lower limits, in the range from -100 to -50 in the unit of dBm.

Defaults

The default is -80 dBm.

Command Mode

Global configuration mode

Usage Guide

This lower limit value is used to differentiate associable STAs from non-associable STAs. If the RSSI value is greater than this value, such STAs are associable and their information will be paid attention to. If the RSSI value is less than this value, the information of such STAs will be ignored. It is not recommended that users modify the default value.

Configuration Examples

The following example sets the acceptable STA RSSI low limit to -70 dBm.

```
FS(config)#band-select acceptable-rssi -70
```

Related Commands

Command	Description
show band-select configuration	Displays the Band Select configuration.

Platform Description

N/A

1.2 band-select access-denial

Use this command to set the access-denial count. Use the **no** form of this command to restore the default setting.

band-select access-denial *value*

no band-select access-denial

Parameter Description

Parameter	Description
value	Sets the access-denial count, in the range from 0 to 10.

Defaults

The default is 2.

Command Mode

Global configuration mode

Usage Guide

The value **n** indicates that the AP does not respond until it receives n consecutive link authentication requests from the dual-band STA on 2.4-GHz band.

> This parameter can increase the navigation rate for high frequency spectrum, but it may cause difficulty in access to some dual-band STAs.

Configuration Examples

The following example sets the access-denial count to 4.

```
FS(config)# band-select access-denial 4
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.3 band-select age-out

Use this command to configure the aging cycle of STA information. Use the **no** form of this command to restore the default setting.

band-select age-out { **dual-band** *value* **|** **suppression** *value* }

no band-select age-out { **dual-band | suppression** }

Parameter Description

Parameter	Description
dual-band *value*	The aging cycle of dual-band STA information, in the range from 20 to 120 in the unit of seconds.
suppression *value*	The aging cycle of suppressed STA information, in the range from 10 to 60 in the unit of seconds.

Defaults

The default aging cycle of dual-band STA information is 60 seconds.

The default aging cycle of suppressed STA information is 20 seconds.

Command Mode

Global configuration mode

Usage Guide

The AP is less sensitive to the STA band switching as the life cycle of the dual-band STA information increases. If the wireless users' network cards often switch between 2.4-GHz and 5-GHz bands, a smaller value can be configured; otherwise, a bigger value can be configured.

It is recommended to configure the aging cycle of dual-band STA information as two or three times as that of the suppressed STAs.

Configuration Examples

The following example sets the aging cycle of dual-band STA information to 120 seconds.

```
FS(config)#band-select age-out dual-band 120
```

The following example sets the aging cycle of suppressed STA information to 60 seconds.

```
FS(config)# band-select age-out suppression 60
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.4 band-select enable

Use this command to enable the spectrum navigation. Use the **no** form of this command to restore the default setting.

band-select enable

no band-select enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

WLAN configuration mode

Usage Guide

Enabling the spectrum navigation requires that:

1. WLAN is mapped to a dual-band AP.

2. WLAN is mapped to two radios of the dual-band AP.

If the scenario cannot meet the above requirements, it is recommended not to enable the spectrum navigation.

If the WLAN with the spectrum navigation enabled is mapped to a single-band 2.4GHz AP, the dual-band STA within AP signal coverage cannot navigate to the 5GHz band.

Configuration Examples

The following example enables the spectrum navigation for WLAN1.

```
FS(config)# wlan-config 1
FS(config-wlan)# band-select enable
```

The following example disables the spectrum navigation for WLAN1.

```
FS(config)# wlan-config 1
FS(config-wlan)# no band-select enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.5 band-select probe-count

Use this command to configure the probe count of the suppressed STAs. Use the **no** form of this command to restore the default setting.

band-select probe-count *value*

no band-select probe-count

Parameter Description

Parameter	Description
value	Indicates the probe-count of the suppressed STAs, in the range is from 1 to 10.

Defaults

The default is 2.

Command Mode

Global configuration mode

Usage Guide

This item indicates the extent of suppression to a suppressed STA: The value **n** indicates that the AP respond once after a STA transmits **n** probe requests.

Configuration Examples

The following example sets the probe count of the suppressed STAs to 1.

```
FS(config)#band-select probe-count 1
```

Related Commands

Command	Description
show band-select configuration	Displays the Band Select configuration.

Platform Description

N/A

1.6 band-select scan-cycle

Use this command to configure the aging scanning cycle of STA information. Use the **no** form of this command to restore the default setting.

band-select scan-cycle *period*

no band-select scan-cycle

Parameter Description

Parameter	Description
period	Indicates the aging scanning cycle, in the range from 1 to 1000 in the unit of milliseconds.

Defaults

The default is 200 milliseconds.

Command Mode

Global configuration mode

Usage Guide

A bigger aging scanning cycle value degrades the Band Select performance, but it can save the system resources.

Configuration Examples

The following example sets the aging scanning cycle to 1 millisecond.

```
FS(config)#band-select scan-cycle 1
```

Related Commands

Command	Description
show band-select configuration	Displays the Band Select configuration.

Platform Description

N/A

1.7 show band-select configuration

Use this command to display the Band Select configuration.

show band-select configuration

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to show all configurations of the Band Select function.

Configuration Examples

The following example displays the Band Select configuration.

```
FS# show band-select configuration
Band Select Configuration
  Band Select Enable................................. Disable
```

```
    Probe Cycle Count....................................... 2
    Scan Cycle Period Threshold (milliseconds)............... 200
    Age Out Suppression (seconds)............................ 20
    Age Out Dual Band (seconds).............................. 60
    Acceptable Client RSSI (dBm)............................ -80
```

Related Commands

Command	Description
show band-select statistics	Displays the Band Select statistics.

Platform Description

N/A

1.8 show band-select statistics

Use this command to display the Band Select statistics.

show band-select statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the Band Select statistics.

Configuration Examples

The following example displays the Band Select statistics.

```
FS# show band-select statistics
Band Select Statistics
    Number of dual band client................................ 4
    Number of dual band client added......................... 132
    Number of dual band client expired....................... 128
    Number of suppressed client.............................. 6
    Number of suppressed client added........................ 234
    Number of suppressed client expired...................... 228
```

Related Commands

Command	Description
show band-select configuration	Displays the Band Select configuration.

Platform

N/A

Description

Chapter 14 WLAN Security Configuration Commands

1 Wireless Security Commands

1.1 authtimeout forbidcount

Use this command to configure the forbidcount after a four-way handshake fails to accomplish key exchange. Use the **no** or **default** form of this command to restore the default setting.

authtimeout forbidcount *count*

no authtimeout forbidcount

default authtimeout forbidcount

Parameter Description

Parameter	Description
count	Sets the forbidcount after a four-way handshake fails to accomplish key exchange.

Defaults The default is 10.

Command mode WLAN security configuration mode

Usage Guide N/A

Configuration Examples The following example sets the forbidcount to 5 after a four-way handshake fails to accomplish key exchange.

```
FS(config-wlansec)#authtimeout forbidcount 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.2 authtimeout forbidtime

Use this command to set the forbidtime after a four-way handshake fails to accomplish key exchange. Use the **no** or **default** form of this command to restore the default setting.

authtimeout forbidtime *time*

no authtimeout forbidtime

default authtimeout forbidtime

Parameter Description

Parameter	Description
time	Sets the forbidtime after a four-way handshake fails to accomplish key exchange, in the unit of seconds.

Defaults

The default is 5.

Command mode

WLAN security configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the forbidtime to 6 seconds after a four-way handshake fails to accomplish key exchange,

```
FS(config-wlansec)#authtimeout forbidtime 6
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.3 authtimeout groupcount

Use this command to set the retransmission count for the multicast key agreement packet. Use the **no** or **default** form of this command to restore the default setting.

authtimeout groupcount *count*

no authtimeout groupcount

default authtimeout groupcount

Parameter Description

Parameter	Description
count	Sets the retransmission count for the multicast key negotiation packet.

Defaults

The default is 7.

Command mode

WLAN security configuration mode

Usage Guide

N/A

Configuration Examples

The following example set the retransmission count for the multicast key negotiation packet to 5.

```
FS(config-wlansec)#authtimeout groupcount 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.4 authtimeout grouptime

Use this command to set the timeout period for the multicast key negotiation packet. Use the **no** or **default** form of this command to restore the default setting.

authtimeout grouptime *timeout*

no authtimeout grouptime

default authtimeout grouptime

Parameter Description

Parameter	Description
timeout	Sets the timeout period for the multicast key negotiation packet, in the unit of milliseconds.

Defaults The default is 1200 milliseconds.

Command mode WLAN security configuration mode

Usage Guide N/A

Configuration Examples The following example sets the timeout period for the multicast key negotiation packet to 100 milliseconds.

```
FS(config-wlansec)#authtimeout grouptime 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.5 authtimeout paircount

Use this command to set the retransmission count for the unicast key negotiation packet. Use the **no** or **default** form of this command to restore the default setting.

authtimeout paircount *count*

no authtimeout paircount

default authtimeout paircount

Parameter Description

Parameter	Description
count	Sets the retransmission count for the unicast key negotiation packet.

Defaults

The default is 7.

Command mode

WLAN security configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the retransmission count for the unicast key negotiation packet to 5.

```
FS(config-wlansec)#authtimeout paircount 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.6 authtimeout pairtime

Use this command to set the timeout period for the unicast key negotiation packet. Use the **no** or **default** form of this command to restore the default setting.

authtimeout pairtime *timeout*

no authtimeout pairtime

default authtimeout pairtime

Parameter Description

Parameter	Description
timeout	Sets the timeout period for the unicast key negotiation packet, in the unit of milliseconds.

Defaults

The default is 1200 milliseconds.

Command mode

WLAN security configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the timeout period for the unicast key negotiation packet to 100 milliseconds.

```
FS(config-wlansec)#authtimeout pairtime 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.7 security rsn

Use this command to configure RSN authentication for a WLAN.

security rsn { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables the RSN authentication mode.
disable	Disables the RSN authentication mode.

Defaults

This function is disabled by default.

Command mode

WLAN security configuration mode

Usage Guide

The command is used to enable the RSN authentication mode. Only after the RSN authentication mode is enabled can encryption and authentication methods be configured in the RSN mode. Otherwise, any configuration is invalid. When you use the RSN authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network. The RSN authentication mode is what is usually called WPA2 authentication mode. If both WPA and RSN authentication modes are configured simultaneously for a WLAN, the encryption and authentication methods in these two authentication modes are identical, and the newly configured encryption and authentication methods will override the previous ones.

Configuration Examples

The following example sets the authentication mode of WLAN1 to RSN.

```
FS(config)#wlansec 1
FS(wlansec)# security rsn enable
```

The following example disables the RSN authentication mode of WLAN1.

```
FS (config)#wlansec 1
FS(wlansec)# security rsn disable
```

Related Commands

Command	Description
security rsn akm { **psk** | **802.1x** } { **enable** | **disable** }	Configures an authentication method in the RSN authentication mode.
security rsn ciphers { **aes** | **tkip** } { **enable** | **disable** }	Configures an encryption method in the RSN authentication mode.
security rsn akm psk set-key ascci	Configures a shared password for RSNs.

Platform

N/A

Description

1.8 security rsn akm

Use this command to configure RSN authentication for a WLAN.

security rsn akm psk { enable | **disable** }

Parameter Description

Parameter	Description
psk	Configures the authentication method to pre-shared key identity verification.
enable	Enables an authentication method in the RSN authentication mode.
disable	Disables an authentication method in the RSN authentication mode.

Defaults N/A

Command mode WLAN security configuration mode

Usage Guide The command is used to enable an authentication method in the RSN authentication mode. Only after the RSN authentication mode is enabled can an authentication method be configured. The authentication method includes PSK.

Configuration Examples The following example configures the authentication method for WLAN1 in the RSN authentication mode to PSK.

```
FS (config)#wlansec 1
FS(wlansec)# security rsn akm psk enable
```

Related Commands

Command	Description
security rsn { **enable** | **disable** }	Configures the WLAN configuration mode.
security rsn ciphers { **aes** | **tkip** } { **enable** | **disable** }	Configures an encryption method in the RSN authentication mode.
security rsn akm psk set-key ascci	Configures a shared password for RSNs.

Platform Description N/A

1.9 security rsn akm psk set-key

Use this command to configure a shared password for RSNs in the PSK authentication mode.

security rsn akm psk set-key { **ascii** *ascii-key* | **hex** *hex-key* }

Parameter Description

Parameter	Description
ascii	Specifies the ASCII password.
ascii-key	The ASCII password, containing 8-63 characters.

hex	Specifies the hexadecimal password.
hex-key	The hexadecimal password, containing 64 characters.

Defaults

N/A

Command mode

WLAN security configuration mode

Usage Guide

This shared password is of use only when the PSK authentication mode is enabled.

Configuration Examples

The following example sets the shared password for WLAN 1 RSN to 12345678.

```
FS (config)#wlansec 1
FS(wlansec)# security rsn enable
FS(wlansec)# security rsn akm psk enable
FS(wlansec)# security rsn akm psk set-key ascci 12345678
```

Related Commands

Command	**Description**
security rsn { **enable** | **disable** }	Configures the RSN authentication mode.
security rsn ciphers { **aes** | **tkip** } { **enable** | **disable** }	Configures an encryption method in the RSN authentication mode.
security rsn akm { **psk** | **802.1x** } { **enable** | **disable** }	Configures an authentication method in the RSN authentication mode.

Platform Description

N/A

1.10 security rsn ciphers

Use this command to configure an encryption method for a WLAN in the RSN authentication mode.

security rsn ciphers { **aes** | **tkip** } { e**nable** | **disable** }

Parameter Description

Parameter	**Description**
aes	Configures the encryption method to AES.
tkip	Configures the encryption method to TKIP.
enable	Enables an encryption method in the RSN authentication mode.
disable	Disables an encryption method in the RSN authentication mode.

Defaults

N/A

Command mode

WLAN security configuration mode

Usage Guide

The command is used to enable an encryption method in the RSN authentication mode. Only after the RSN authentication mode is enabled can an encryption method be configured. There are two encryption methods: AES and TKIP. When you use the RSN authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network. The RSN authentication mode is what is usually called WPA2 authentication mode. If both WPA and RSN authentication modes are configured simultaneously for a WLAN, the encryption and authentication methods in these two authentication modes are identical, and the newly configured encryption and authentication methods will override the previous ones. AES encryption must be enabled if you want to enable 802.11r.

Configuration Examples

The following example configures the encryption method for WLAN1 in the RSN authentication mode to AES.

```
FS (config)#wlansec 1
FS(wlansec)# security rsn ciphers aes enable
```

The following example disables the AES encryption method for WLAN1 in the RSN authentication mode.

```
FS (config)#wlansec 1
FS(wlansec)# security wpa ciphers aes disable
```

The following example sets the encryption method for WLAN1 in the RSN authentication mode to TKIP.

```
FS (config)#wlansec 1
FS(wlansec)# security rsn ciphers tkip enable
```

The following example disables the TKIP encryption method for WLAN1 in the RSN authentication mode.

```
FS (config)#wlansec 1
FS(wlansec)# security rsn ciphers tkip disable
```

Related Commands

Command	Description
security rsn { **enable** | **disable** }	Configures the RSN authentication mode.
security rsn akm { **psk** | **802.1x** } { **enable** | **disable** }	Configures an authentication method in the RSN authentication mode.
security rsn akm psk set-key ascci	Configures a shared password for RSNs.

Platform Description

N/A

1.11 security static-wep-key authentication

Use this command to configure an authentication method for a WLAN in the static WEP mode.

security static-wep-key authentication { **open** | **share-key** }

Parameter Description

Parameter	Description
open	The open system authentication mode.
share-key	The shared key authentication mode.

Defaults

The default is **open**.

Command mode

WLAN security configuration mode

Usage Guide

This command must be used with the **security static-wep-key encryption** command. Usually, the static WEP key must be configured before the shared key authentication method can be configured. In any security mode other than the static WEP security mode, it is of no use to configure the link authentication mode.

Configuration Examples

The following example sets the authentication mode of WLAN1 to open system authentication.

```
FS (config)#wlansec 1
FS(wlansec)# security static-wep-key authentication open
```

The following example sets the authentication mode of WLAN1 to shared key authentication.

```
FS (config)#wlansec 1
FS(wlansec)# security static-wep-key authentication share-key
```

Related Commands

Command	Description
security static-wep-key encryption	Configures the static WEP key, and enables the static WEP security mode.

Platform Description

N/A

1.12 security static-wep-key encryption

Use this command to configure the static WEP key for a WLAN and configure the security mode of this WLAN to static WEP.

security static-wep-key encryption *key-length* { **ascii** | **hex** } *key-index key*

Parameter Description

Parameter	Description
key-length	The key length is measured by bit, which can be 40, 104, and 128 bits.
key-index	The parameter indicates a key index number, ranging from 1 to 4.
key	The parameter indicates key data. In the ascii mode, 5-byte, 13-byte, and 16-byte data can serve as a key depending on the **key-length** parameter. In the hex mode, 10-byte, 26-byte, and 32-byte data can serve as a key depending on the **key-length** parameter.
ascii	The parameter indicates that the password takes the form of ASCII code.
hex	The parameter indicates that the password is hexadecimal.

Defaults

The static WEP mode is disabled by default.

Command mode

WLAN security configuration mode

Usage Guide

The prerequisite of configuring security mode for a WLAN is that this WLAN has been created. Attention should be paid to the following points:

1. This command can be used repeatedly for configuration, and the last configuration will take effect.
2. This command configures the static WEP key as well as the static-WEP security mode.

Configuration Examples

The following example sets the static WEP key of WLAN 1 to 12345.

```
FS (config)#wlansec 1
FS(wlansec)# security static-wep-key encryption 40 ascii 1 12345
```

Related Commands

Command	Description
security static-wep-key authentication { **open** | **share-key** }	Configures the authentication method in the static WEP security mode to open system authentication or shared key authentication.

Platform Description

The client cannot support a 128-bit WEP password if you use the Windows XP operating system in the wireless client management software. If the client software does not support a 128-bit WEP password, as FS devices are configured with 128-bit encryption, the consequence is either the client software cannot be associated with the wireless network or the data channel is unavailable, depending on the authentication mode.

1.13 security wpa

Use this command to configure WPA authentication for a WLAN.

security wpa { **enable** | **disable** }

Parameter Description

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 command is used to enable the WPA authentication mode. Only after the WPA authentication mode is enabled can encryption and authentication methods be configured in the WPA mode. Otherwise, configuration is impossible. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

Configuration

The following example sets the authentication mode of WLAN1 to WPA.

Examples

```
FS (config)#wlansec 1
FS(wlansec)# security wpa enable
```

The following example disables the WPA authentication of WLAN1.

```
FS (config)#wlansec 1
FS(wlansec)# security wpa disable
```

Related Commands

Command	Description
security wpa akm { **psk** | **802.1x** } { **enable** | **disable** }	Configures an authentication method in the WPA authentication mode.
security wpa ciphers { **aes** | **tkip** } { **enable** | **disable** }	Configures an encryption method in the WPA authentication mode.
security wpa akm psk set-key ascci	Configures the shared password in the WPA authentication mode.

Platform Description

N/A

1.14 security wpa akm

Use this command to configure an authentication method for a WLAN in the WPA authentication mode.

security wpa akm { **psk** | **802.1x** } { **enable** | **disable** }

Parameter Description

Parameter	Description
psk	Configures the authentication method to pre-shared key identity verification.
enable	Enables an authentication method in the WPA authentication mode.
disable	Disables an authentication method in the WPA authentication mode.

Defaults

N/A

Command mode

WLAN security configuration mode

Usage Guide

The command is used to enable an authentication method in the WPA authentication mode. Only after the WPA authentication mode is enabled can an authentication method be configured. Authentication method includes PSK. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

Configuration Examples

The following example sets the authentication method for WLAN1 in the WPA authentication mode to pre-shared key identity authentication.

```
FS (config)#wlansec 1
FS(wlansec)# security wpa akm psk enable
```

Related Commands

Command	Description
security wpa { **enable** | **disable** }	Configures the WLAN configuration mode.
security wpa ciphers { **aes** | **tkip** } { **enable** | **disable** }	Configures an encryption method in the WPA authentication mode.

Platform Description N/A

1.15 security wpa akm psk set-key ascci

Use this command to configure a WPA shared password for a WLAN.

security wpa akm psk set-key { **ascii** *ascii-key* | **hex** *hex-key* }

Parameter Description

Parameter	Description
ascii	Specifies the ASCII password.
ascii-key	The ASCII password, containing 8-63 characters.
hex	Specifies the hexadecimal password.
hex-key	The hexadecimal password, containing 64 characters.

Defaults N/A

Command mode WLAN security configuration mode

Usage Guide This shared password is of use only when the PSK authentication mode is enabled.

Configuration Examples The following example sets the shared password for WLAN 1 WPA to 12345678.

```
FS (config)#wlansec 1
FS(wlansec)# security wpa enable
FS(wlansec)# security wpa akm psk enable
FS(wlansec)# security wpa akm psk set-key ascci 12345678
```

Related Commands

Command	Description
security wpa { **enable** | **disable** }	Configures the WLAN configuration mode.
security wpa ciphers { **aes** | **tkip** } { **enable** | **disable** }	Configures an encryption method in the WPA authentication mode.
security wpa akm { **psk** | **802.1x** } { **enable** | **disable** }	Configures an authentication method in the WPA authentication mode.

Platform N/A

Description

1.16 security wpa ciphers

Use this command to configure an encryption method for a WLAN in the WPA authentication mode.

security wpa ciphers { **aes** | **tkip** } { **enable** | **disable** }

Parameter Description

Parameter	Description
aes	Configures the encryption method to AES.
tkip	Configures the encryption method to TKIP.
enable	Enables an encryption method in the WPA authentication mode.
disable	Disables an encryption method in the WPA authentication mode.

Defaults

N/A

Command mode

WLAN security configuration mode

Usage Guide

The command is used to enable an encryption method in the WPA authentication mode. Only after the WPA authentication mode is enabled can an encryption method be configured. There are two encryption methods: AES and TKIP. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

Configuration Examples

The following example sets the encryption method for WLAN1 in the WPA authentication mode to AES.

```
FS (config)#wlansec 1
FS(wlansec)# security wpa ciphers aes enable
```

The following example disables the AES encryption method for WLAN1 in the WPA authentication mode.

```
FS (config)#wlansec 1
FS(wlansec)# security wpa ciphers aes disable
```

The following example sets the encryption method for WLAN1 in the WPA authentication mode to TKIP.

```
FS (config)#wlansec 1
FS(wlansec)# security wpa ciphers tkip enable
```

The following example disables the TKIP encryption method for WLAN1 in the WPA authentication mode.

```
FS (config)#wlansec 1
FS(wlansec)# security wpa ciphers tkip disable
```

Related Commands

Command	Description
security wpa { **enable** | **disable** }	Configures the WLAN configuration mode.
security wpa akm { **psk** | **802.1x** } { **enable** | **disable** }	Configures an authentication method in the WPA authentication mode.
security wpa akm psk set-key ascci	Configures a shared password in the WPA

	authentication mode.

Platform Description N/A

1.17 webauth prevent-jitter

Use this command to set the timeout for jitter prevention during Web authentication of a particular WLAN. Use the **no** or **default** form of this command to restore the default setting.

webauth prevent-jitter *timeout*

no webauth prevent-jitter

default webauth prevent-jitter

Parameter Description

Parameter	Description
timeout	Sets the timeout for jitter prevention during Web authentication, in the range from 0 to 86400 in the unit of seconds.

Defaults The default is 300 seconds.

Command mode WLAN security configuration mode

Usage Guide N/A

Configuration Examples The following example sets the timeout for jitter prevention during Web authentication of WLAN 1 to 900 seconds.

```
FS(config)#wlansec 1
FS(config-wlansec)#webauth
FS(config-wlansec)#webauth prevent-jitter 900
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.18 wlansec

Use this command to configure security configuration mode for the specified WLAN. Use the **no** or **default** form of this command to restore the default setting.

wlansec *wlan-id*

no wlansec *wlan-id*

default wlansec *wlan-id*

Parameter Description

Parameter	Description
wlan-id	Sets WLAN ID.

Defaults

No WLAN security configuration mode is configured by default.

Command mode

Global configuration mode

Usage Guide

Create a WLAN before entering its security configuration mode. You can use the **no wlansec** *wlan-id* command to clear the WLAN security configuration.

Configuration Examples

The following example configures security configuration mode for WLAN 1.

```
FS(config)#wlansec 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.19 show wlan security

Use this command to display security configuration of a WLAN.

show wlan security *wlan-id*

Parameter Description

Parameter	Description
wlan-id	The ID of the WLAN to be checked, in the range from 1 to 512.

Defaults

N/A

Command mode

Privileged EXEC mode/Global configuration mode/WLAN security configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the security configuration of WLAN1.

```
FS#show wlan security 1
WLAN SSID                    : FS-psk
Security Policy         : PSK
WPA version                  : RSN(WPA2)
```

```
AKM type                 : preshare key
pairwise cipher type: AES
group cipher type      : AES
wpa_passphrase_len    : 8
wpa_passphrase          : 31 32 33 34 35 36 37 38
group key                  : 39 de c7 57 5c 58 9a af 84 84 cf 18 3e ce ff 5c
```

Field	Description
WLAN SSID	WLAN SSID
Security Policy	Security policy
WPA version	WPA version.
AKM type	AKM suite, indicating the authentication mode.
pairwise cipher type	Unicast cipher suite.
group cipher type	Multicast cipher suite.
wpa_passphrase_len	Password length.
wpa_passphrase	PSK password.
group key	Multicast key.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.20 show wclient security

Use this command to display security configuration of STAs.

show wclient security *mac-address*

Parameter Description

Parameter	Description
mac-address	The MAC address of the STA to be displayed.

Defaults

N/A

Command mode

Privileged EXEC mode/Global configuration mode/WLAN security configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the security configuration of wireless client 1 with a MAC address of 3848.4c48.d953.

```
FS# show wclient security 3848.4c48.d953
```

```
Security policy finished          :TRUE
Security policy type                :PSK
Security WPA version                  :WPA2
Security Ucast cipher                :CCMP
Security EAP type                       :NONE
```

Field	Description
Security policy finished	Whether the authentication is complete.
Security policy type	Security policy type.
Security WPA version	WPA version.
Security Ucast cipher	Unicast cipher suite
Security EAP type	EAP Type

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2 WIDS Commands

2.1 attack-detection enable

Use this command to enable the IDS attack detection. Use the **no** form of this command to restore the default setting.

attack-detection enable { **all** | **flood** | **ddos** | **spoof** | **weak-iv** }

no attack-detection enable { **all** | **flood** | **ddos** | **spoof** | **weak-iv** }

Parameter Description

Parameter	Description
all	Enables all types of IDS attack detection.
flood	Enables the Flooding IDS attack detection.
weak-iv	Enables the Weak-IV IDS attack detection.
spoof	Enables the Spoofing IDS attack detection.
ddos	Enables the DDOS IDS attack detection.

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example enables the Flooding IDS attack detection.

```
FS(config-wids)# attack-detection enable flood
```

The following example disables the Flooding IDS attack detection.

```
FS(config-wids)#no attack-detection enable flood
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.2 attack-detection ddos

Use this command to specify the packet threshold and interval for DDOS attack detection. Use the **no** form of this command to restore the default setting.

attack-detection ddos { **arp-threshold** *num* | **icmp-threshold** *num* | **syn-threshold** *num* | **interval** *time* }

no attack-detection ddos { **arp-threshold** | **icmp-threshold** | **syn-threshold** | **interval** }

Parameter Description

Parameter	Description
interval *time*	DDOS detection interval in the range from 10 to 60 in the unit of seconds.
arp-threshold *num*	ARP packet threshold in the range from 1 to 10000 in the unit of pps.
icmp-threshold *num*	ICMP packet threshold in the range from 1 to 10000 in the unit of pps.
syn-threshold *num*	SYN packet threshold in the range from 1 to 10000 in the unit of pps.

Defaults

The **arp-threshold** is 5pps, **icmp-threshold** is 100pps, **syn-threshold** is 5pps, and **interval** is 30 seconds by default.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets ARP packet threshold to 200pps for DDOS attack detection.

```
FS(config-wids)# attack-detection ddos arp-threshold 200
```

The following example restores ARP packet threshold to the default setting.

```
FS(config-wids)#no attack-detection ddos arp-threshold
```

Platform Description

N/A

2.3 attack-detection flood multi-mac

Use this command to specify the packet threshold and interval for Flooding attack detection in a multi-user system. Use the **no** form of this command to restore the default setting.

attack-detection flood multi-mac { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth | null-data** } **threshold** *num* **interval** *time*

no attack-detection flood multi-mac { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth | null-data** }

Parameter Description

Parameter	Description
assoc	Specifies the association packet.
reassoc	Specifies the reassocation packet.
disassoc	Specifies the disassociation packet.
probe	Specifies the probe request packet.
action	Specifies the action packet.
auth	Specifies the authentication packet.
deauth	Specifies the deauthentication packet.
null-data	Specifies the null data packet.
threshold *num*	Packet threshold in the range from 1 to 5,000.
interval *time*	Statistics interval threshold in the range from 10 to 60 in the unit of seconds.

Defaults The **threshold** is 500 and the **interval** is 10 seconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets **assoc** to 200 and **interval** to 20000ms for Flooding attack detection in a multi-user system.

```
FS(config-wids)# attack-detection flood multi-mac assoc threshold 200 interval 20000
```

The following example restores **assoc** and **interval** to the default setting.

```
FS(config-wids)#no attack-detection flood multi-mac assoc
```

Platform Description N/A

2.4 attack-detection flood single-mac

Use this command to set the packet threshold and statistics interval for Flooding attack detection in a single-user system. Use the **no** form of this command to restore the default setting.

attack-detection flood single-mac { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth |** **null-data** } **threshold** *num* **interval** *time*

no attack-detection flood single-mac { **tota** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth |** **null-data** }

Parameter Description

Parameter	Description
total	Specifies all types of packets.
assoc	Specifies the association packet.
reassoc	Specifies the reassocation packet.
disassoc	Specifies the disassociation packet.
probe	Specifies the probe request packet.
action	Specifies the action packet.
auth	Specifies the authentication packet.
deauth	Specifies the deauthentication packet.
null-data	Specifies the null data packet
threshold *num*	Packet threshold in the range from 1 to 5000.
interval *time*	Statistics interval threshold in the range from 10 to 60 in the unit of seconds.

Defaults The **threshold** is 300 and the **interval** is 10 seconds by default.

Command WIDS configuration mode

Mode

Usage Guide N/A

Configuration Examples The following example sets **assoc** to 200 and **interval** to 20000 milliseconds for Flooding attack detection in a single-user system.

```
FS(config-wids)# attack-detection flood single-mac assoc threshold 200 interval 20000
```

The following example restores **assoc** and **interval** to the default setting.

```
FS(config-wids)#no attack-detection flood single-mac assoc
```

Platform Description N/A

2.5 attack-detection spoof

Use this command to set the packet threshold and statistics interval for Spoofing attack detection. Use the **no** form of this command to restore the default setting.

attack-detection spoof { **threshold** *num* **|** **interval** *time* }

no attack-detection spoof { **threshold** | **interval** }

Parameter Description

Parameter	Description
threshold *num*	Packet threshold in the range from 1 to 1000.
interval *time*	Detection interval in the range from 10 to 60 in the unit of seconds.

Defaults The **threshold** is 1 second and the **interval** is 50 seconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the packet threshold for Spoofing attack detection to 20.

```
FS(config-wids)# attack-detection spoof threshold 20
```

The following example restores the ARP packet threshold for Spoofing attack detection to the default setting.

```
FS(config-wids)#no attack-detection spoof threshold
```

Platform Description N/A

2.6 attack-detection weak-iv

Use this command to set the packet threshold and interval for Weak IV attack. Use the **no** form of this command to restore the default setting.

attack-detection weak-iv { **threshold** *num* **|** **interval** *time* }

no attack-detection weak-iv { **threshold** | **interval** }

Parameter Description

Parameter	Description
threshold *num*	Packet threshold in the range from 1 to 10000.
interval *time*	Detection interval in the range from 1 to 60 in the unit of seconds.

Defaults The **threshold** is 10 seconds and the **interval** is 15 seconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples

The following example sets the packet threshold for Weak IV attack detection to 200.

```
FS(config-wids)# attack-detection weak-iv threshold 200
```

The following example restores the packet threshold for Weak IV attack to the default setting.

```
FS(config-wids)#no attack-detection weak-iv threshold
```

Platform Description N/A

2.7 attack-detection statistics ac-max

Use this command to configure the maximum number of IDS attack detection lists on the AC. Use the **no** form of this command to restore the default setting.

attack-detection statistics ac-max *num*

no attack-detection statistics ac-max

Parameter Description

Parameter	Description
num	The maximum number of IDS attack detection lists on the AC in the range from 1 to 4096.

Defaults The default is 2048.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples

The following example configures the maximum number of the IDS attack detection list to 2000.

```
FS(config-wids)# attack-detection statistics ac-max 2000
```

The following example restores the maximum number of the IDS attack detection list to the default setting.

```
FS(config-wids)#no attack-detection statistics ac-max
```

Platform Description

N/A

2.8 attack-detection statistics ap-max

Use this command to configure the maximum number of IDS attack detection lists on the AP. Use the **no** form of this command to restore the default setting.

attack-detection statistics ap-max *num*

no attack-detection statistics ap-max

Parameter Description

Parameter	Description
num	The maximum number of IDS attack detection lists on the AP in the range from 1 to 1024.

Defaults

The default is 512.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the maximum number of IDS attack detection lists on the AC to 1000.

```
FS(config-wids)# attack-detection statistics ap-max 1000
```

The following example restores the maximum number of IDS attack detection lists to the default setting.

```
FS(config-wids)#no attack-detection statistics ap-max
```

Platform Description

N/A

2.9 countermeasures ap-max

Use this command to configure the maximum number of APs for the countermeasures.

Use the **no** form of this command to restore the default setting.

countermeasures ap-max *ap-num*

no countermeasures ap-max

Parameter

Parameter	Description

Description

ap-num	Specifies the maximum number of APs for the countermeasures in the range from 1 to 256.

Defaults The default is 30.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of APs for the countermeasures to 22.

```
FS(config-wids)# countermeasures ap-max 22
```

The following example restores the maximum number of APs for the countermeasures to the default setting.

```
FS(config-wids)#no countermeasures ap-max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.10 countermeasures enable

Use this command to enable the device countermeasures. Use the **no** form of this command to restore the default setting.

countermeasures enable

no countermeasure enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide This command does not take effect in AP normal working mode.

Configuration Examples The following example enables the device countermeasures.

```
FS(config-wids)#countermeasures enable
```

The following example disables the device countermeasures.

```
FS(config-wids)#no countermeasures enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.11 countermeasures channel-match

Use this command to enable the channel-based countermeasures. Use the **no** form of this command to restore the default setting.

countermeasures channel-match

no countermeasures channel-match

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

WIDS configuration mode

Usage Guide

Use this command after the device countermeasures are enabled.

Configuration Examples

The following example enables the channel-based countermeasures.

```
FS(config-wids)# countermeasures channel-match
```

The following example disables the channel-based countermeasures.

```
FS(config-wids)#no countermeasures channel-match
```

Platform Description

N/A

2.12 countermeasures interval

Use this command to set the device countermeasures interval. Use the **no** form of this command to restore the default setting.

countermeasures interval *time*

no countermeasures interval

Parameter Description

Parameter	Description
time	Device countermeasures interval in the range from 100 to 10000 in the unit of milliseconds.

Defaults

The default is 1000 milliseconds.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the countermeasures interval to 2000 milliseconds.

```
FS(config-wids)# countermeasures interval 2000
```

The following example restores the countermeasures interval to the default setting.

```
FS(config-wids)#no countermeasures interval
```

Platform Description

N/A

2.13 countermeasures mode

Use this command to configure the device countermeasures mode. Use the **no** form of this command to restore the default setting.

countermeasures mode { **all** | **adhoc** | **config** | **rogue** | **ssid** }

no countermeasures mode { **all** | **adhoc** | **config** | **rogue** | **ssid** }

Parameter Description

Parameter	Description
all	Indicates all countermeasures are enabled.
ssid	Indicates the devices with the same SSID on the AP are subjected to the countermeasures.
rogue	Indicates only detected rogue devices are subjected to the countermeasures.
adhoc	Indicates only detected adhoc devices are subjected to the countermeasures.
config	Indicates only the devices configured in the static attack list are subjected to the countermeasures.

Defaults

This function is disabled by default.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the device countermeasures mode to **adhoc**.

```
FS(config-wids)# countermeasure mode adhoc
```

The following example disables the **adhoc** mode.

```
FS(config-wids)#no countermeasures mode adhoc
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.14 countermeasures rssi-min

Use this command to configure the lower limit of the signal for the countermeasures.

Use the **no** form of this command to restore the default setting.

countermeasures rssi-min *num*

no countermeasures rssi-min

Parameter Description

Parameter	Description
num	Specifies the lower limit of the signal strength for the countermeasures in the range from 0 to 75 (-95 to -20).

Defaults

The default is 25 (-70).

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the lower limit of the signal strength for the countermeasures to 40.

```
FS(config-wids)# countermeasures rssi-min 40
```

The following example restores the default setting.

```
FS(config-wids)#no countermeasures rssi-min
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

2.15 device aging duration

Use this command to configure device aging duration. Use the **no** form of this command to restore the default setting.

device aging duration *time*

no device aging duration

Parameter Description

Parameter	Description
time	Indicates device aging duration in the range from 500 to 5000 in the unit of seconds.

Defaults The default is 1200 seconds.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the device aging duration to 1000 seconds.

```
FS(config-wids)# device aging duration 1000
```

The following example restores the device aging duration to the default setting.

```
FS(config-wids)#no device aging duration
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.16 device attack mac-address

Use this command to configure an entry for static attack list. Use the **no** form of this command to delete a configured entry of the static attack list.

device attack mac-address *H.H.H*

no device attack mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates the device with this source MAC address is subjected to the countermeasures.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This configuration is one of the policies for detecting Rogue devices.

Configuration Examples The following example configures the device with the static attack source MAC address of 0000.0000.0001.

```
FS(config-wids)# device attack mac-address 0000.0000.0001
```

The following example deletes the static attack list with its source MAC address of 0000.0000.0001.

```
FS(config-wids)#no device attack mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.17 device attack max

Use this command to configure the maximum number of the static attack list.

Use the **no** form of this command to restore the default setting.

device attack max *num*

no device attack max

Parameter Description

Parameter	Description
num	Specifies the maximum number of the static attack list in the range from 1 to 1024.

Defaults The default is 512.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the static attack list to 900.

```
FS(config-wids)# device attack max 900
```

The following example restores the default setting.

```
FS(config-wids)#no device attack max
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.18 device black-ssid

Use this command to configure an entry for the SSID blacklist. Use the **no** form of this command to remove an entry from the SSID blacklist.

device black-ssid *ssid*

no device black-ssid *ssid*

Parameter Description

Parameter	Description
ssid	The SSID configured to the blacklist. The detection device detects this SSID for countermeasures in WIDS config mode,

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures SSID: my-vlan to the SSID blacklist.

```
FS(config-wids)# device black-ssid my-wlan
```

The following example removes SSID: my-vlan from the SSID blacklist.

```
FS(config-wids)#no device black-ssid my-wlan
```

Platform Description

N/A

2.19 device channel-bind

Use this command to configure channel scan for a specified radio. Use the **no** form of this command to restore the default setting.

device channel-bind radio *radio-id* { **channel** *num* | **max-cycles** *value* }

no device channel-bind radio *radio-id*

Parameter

Parameter	Description

Description

radio *radio-id*	Radio ID.
channel *num*	Channel number in the range from 1 to 255.
max-cycles *value*	Scan cycle in the range from 0 to 255.

Defaults

The **channel** is CCnet and the **max-cycles** is 10 by default.

Command Mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the scan cycle to 20.

```
FS#configure
FS(config)#ap-config ap1
FS(config-ap)#device channel-bind radio 1 max-cycles 20
```

Platform Description

N/A

2.20 device detected-ap-max

Use this command to configure the maximum number of detected AP list members. Use the **no** form of this command to restore the default setting.

device detected-ap-max *num*

no device detected-ap-max *num*

Parameter Description

Parameter	Description
detected-ap-max *num*	The maximum number of detected AP list members.

Defaults

The default is 2048.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the maximum number of detected AP list members to 1000.

```
FS#configure
FS(config)#wids
FS(config-wids)#device detected-ap-max 1000
```

Platform

N/A

Description

2.21 device friendly-flags

Use this command to configure the friendly flag on a device. Use the **no** form of this command to restore the default setting.

device friendly-flags *value*

no device friendly-flags

Parameter Description

Parameter	Description
value	Friendly flag value in the range from 1 to 4294967295.

Defaults The default is 0.

Command Mode WIDS configuration mode

Usage Guide By configuring the friendly flag, AC/AP is able to recognize a friendly AP. The default is random configuration.

Configuration Examples The following example configures the friendly flag to 4294967295.

```
FS(config-wids)# device friendly-flags 4294967295
```

The following example restores the friendly flag to the default setting.

```
FS(config-wids)#no device friendly-flags
```

Platform Description N/A

2.22 device max-black-ssid

Use this command to configure the maximum number of the SSID blacklist. Use the **no** form of this command to restore the default setting.

device max-black-ssid *num*

no device max-black-ssid

Parameter Description

Parameter	Description
num	The maximum number of the SSID blacklist in the range from 1 to 1024.

Defaults The default is 512.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples

The following example configures the maximum number of the SSID blacklist to 900.

```
FS(config-wids)# device max-black-ssid 900
```

The following example restores the default setting.

```
FS(config-wids)#no device max-black-ssid
```

Platform Description N/A

2.23 device mode

Use this command to configure the working mode of the AP. Use the **no** form of this command to restore the default setting.

device mode { **monitor** | **normal** | **hybrid** }

no device mode

Parameter Description

Parameter	Description
monitor	Indicates AP works in the monitor mode.
normal	Indicates AP works in the normal mode.
hybrid	Indicates AP works in the hybrid mode.

Defaults The AP works in the normal mode by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example sets the working mode of the AP to **hybrid**.

```
FS#configure
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#ap-config ap1
FS(config-ap)#device mode hybrid
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.24 device permit mac-address

Use this command to configure an entry for the permissible MAC address list. Use the **no** form of this command to delete an entry from the permissible MAC address list.

device permit mac-address *H.H.H*

no device permit mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates the device with this source MAC address is legal.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This configuration is one of the policies for detecting rogue devices.

Configuration Examples

The following example configures the device with the permissible source MAC address of 0000.0000.0001.

```
FS(config-wids)# device permit mac-address 0000.0000.0001
```

The following example deletes the device with the permissible source MAC address of 0000.0000.0001.

```
FS(config-wids)#no device permit mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.25 device permit mac-address max

Use this command to configure the maximum number of the permissible MAC address list.

Use the **no** form of this command to restore the default setting.

device permit mac-address max *num*

no device permit mac-address max

Parameter Description

Parameter	Description
num	Specifies the maximum number of the permissible MAC address list in the range from 1 to 2048.

Defaults The default is 1024.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the maximum number of the permissible MAC address list to 1000.

```
FS(config-wids)# device permit mac-address max 1000
```

The following example restores the default setting.

```
FS(config-wids)#no device permit mac-address max
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.26 device permit ssid

Use this command to configure an entry for the permissible SSID list. Use the **no** form of this command to delete an entry for the permissible SSID list.

device permit ssid *ssid*

no device permit ssid *ssid*

Parameter Description

Parameter	Description
ssid	Configures this SSID to the permissible SSID list.

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

This configuration is one of the policies for detecting rogue devices.

Configuration Examples

The following example configures SSID: my-wlan to the permissible SSID list.

```
FS(config-wids)# device permit ssid my-wlan
```

The following example removes SSID: my-wlan from the permissible SSID list.

```
FS(config-wids)#no device permit ssid my-wlan
```

Platform

N/A

Description

2.27 device permit max-ssid

Use this command to configure the maximum number of the permissible SSID list members.

Use the **no** form of this command to restore the default setting.

device permit max-ssid *num*

no device permit max-ssid

Parameter Description

Parameter	Description
num	Specifies the maximum number of permissible SSID list members in the range from 1 to 1024.

Defaults The default is 512.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of the permissible SSID list members to 900.

```
FS(config-wids)# device permit max-ssid 900
```

The following example restores the default setting.

```
FS(config-wids)#no device permit max-ssid
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.28 device permit vendor bssid

Use this command to configure an entry for the permissible vendor list. Use the **no** form of this command to delete an entry for the permissible vendor list.

device permit vendor bssid *H.H.H*

no device permit vendor bssid *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates this vendor’s address is a permissible address.

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

The vendor number is used to configure the first three bytes of a MAC address. Do not configure multiple MAC addresses with the same vendor number. This configuration is one of the policies for detecting Rogue devices.

Configuration Examples

The following example configures the MAC address 0000.0000.0001 into the permissible vendor list.

```
FS(config-wids)# device permit vendor bssid 0000.0000.0001
```

The following example deletes the MAC address 0000.0000.0001 from the permissible vendor list.

```
FS(config-wids)#no device permit vendor bssid 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.29 device permit vendor bssid max

Use this command to configure the maximum number of the permissible vendor list members.

Use the **no** form of this command to restore the default setting.

device permit vendor bssid max *num*

no device permit vendor bssid max

Parameter Description

Parameter	Description
num	Specifies the maximum number of the permissible vendor list members in the range from 1 to 1024.

Defaults

The default is 512.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the maximum number of the permissible vendor list members to 1000.

```
FS(config-wids)# device permit vendor bssid max 1000
```

The following example restores the default setting.

```
FS(config-wids)#no device permit vendor bssid max
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.30 device scan-para

Use this command to configure Rogue AP detection parameters according to *CMCC WLAN AC-AP Interoperability Specification*.

device scan-para { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* }

no device scan-para { **radio** *radio-id* | **ap-mode** | **detect-rpt-time** }

Parameter Description

Parameter	Description
radio *radio-id*	Radio ID.
scan-type active	Scan type: active.
scan-type passive	Scan type: passive.
device-detect enable	Enables detection.
device-detect disable	Disables detection.
ap-mode normal	AP operation mode: normal mode.
ap-mode monitor	AP operation mode: monitor mode.
detect-rpt-time *time*	Detection report interval in the range from 60 to 120 in the unit of seconds.

Defaults

The scan type is passive, detection is disabled and detection report interval is 60 seconds by default.

Command Mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example restores for Rogue AP detection type and status to the default setting according to *CMCC WLAN AC-AP Interoperability Specification*.

```
FS#configure
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#ap-config ap1
FS(config-ap)#no device scan-para radio 1
```

Platform Description

N/A

2.31 device unknown-sta dynamic-enable

Use this command to enable dynamic unknown STA detection. Use the **no** form of this command to restore the default setting.

device unknown-sta dynamic-enable

no device unknown-sta dynamic-enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide This command takes effect only when the AP works in the normal mode,

Configuration Examples The following example enables dynamic unknown STA detection.

```
FS(config-wids)# device unknown-sta dynamic-enable
```

The following example disables dynamic unknown STA detection.

```
FS(config-wids)#no device unknown-sta dynamic-enable
```

Platform Description N/A

2.32 device unknown-sta mac-address

Use this command to configure an entry for the static unknown STA list. Use the **no** form of this command to delete an entry for the static unknown STA list.

device unknown-sta mac-address *H.H.H*

no device unknown-sta mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates that the user of this MAC address is unknown STA.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This command is one of the policies for detecting Rogue devices.

Configuration Examples

The following example configures the MAC address 0000.0000.0001 to the unknown STA list.

```
FS(config-wids)# device unknown-sta mac-address 0000.0000.0001
```

The following example removes the MAC address 0000.0000.0001 from the unknown STA list.

```
FS(config-wids)#no device unknown-sta mac-address 0000.0000.0001
```

Platform Description

N/A

2.33 device unknown-sta mac-address max

Use this command to configure the maximum number of the unknown STA list members. Use the **no** form of this command to restore the default setting,

device unknown-sta mac-address max *num*

no device unknown-sta mac-address max

Parameter Description

Parameter	Description
num	The maximum number of the unknown STA list members in the range from 1 to 256.

Defaults

The default is 128.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the maximum number of the unknown STA list members to 200.

```
FS(config-wids)# device unknown-sta mac-address max 200
```

The following example restores the maximum number of the unknown STA list members to the default setting.

```
FS(config-wids)#no device unknown-sta mac-address max
```

Platform Description

N/A

2.34 dos-detection

Use this command to enable DOS attack detection and its threshold according to *CMCC WLAN AC-AP Interoperability Specification*. Use the **no** form of this command to restore the default setting.

dos-detection { **enable** | **threshold** *num* | **interval** *time* }

no dos-detection { **enable** | **threshold** | **interval** }

Parameter

Parameter	Description

Description

enable	Enables DOS attack detection.
threshold *num*	Packet threshold in the range from 1 to 5000.
Interval *time*	Detection interval in the range from 1 to 60000 in the unit of milliseconds.

Defaults This function is disabled, **threshold** is 30, and **interval** is 1000 milliseconds by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example enable DOS attack detection according to *CMCC WLAN AC-AP Interoperability Specification*.

```
FS(config-wids)#dos-detection enable
```

Platform Description N/A

2.35 dynamic-blacklist enable

Use this command to enable the dynamic blacklist. Use the **no** form of this command to restore the default setting.

dynamic-blacklist enable

no dynamic-blacklist enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example enables the dynamic blacklist.

```
FS(config-wids)# dynamic-blacklist enable
```

The following example disables the dynamic blacklist.

```
FS(config-wids)#no dynamic-blacklist enable
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

2.36 dynamic-blacklist lifetime

Use this command to configure the dynamic blacklist entry lifetime. Use the **no** form of this command to restore the default setting.

dynamic-blacklist lifetime *time*

no dynamic-blacklist lifetime

Parameter Description

Parameter	Description
time	Indicates the dynamic blacklist entry lifetime in the range from 60 to 1200 in the unit of seconds.

Defaults The default is 300 seconds.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the dynamic blacklist entry lifetime to 600 seconds.

```
FS(config-wids)# dynamic-blacklist lifetime 600
```

The following example restores the default setting.

```
FS(config-wids)#no dynamic-blacklist lifetime
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.37 dynamic-blacklist ac-max

Use this command to configure the maximum number of the dynamic blacklist members on the AC. Use the **no** form of this command to restore the default setting.

dynamic-blacklist ac-max *num*

no dynamic-blacklist ac-max

Parameter

Parameter	Description

Description

num	The maximum number of the dynamic blacklist members on the AC in the range from 1 to 4096.

Defaults

The default is 2048.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the maximum number of the dynamic blacklist members on the AC to 2000.

```
FS(config-wids)# dynamic-blacklist ac-max 2000
```

The following example restores the default setting.

```
FS(config-wids)#no dynamic-blacklist ac-max
```

Platform Description

N/A

2.38 dynamic-blacklist ap-max

Use this command to configure the maximum number of dynamic blacklist members on the AP. Use the **no** form of this command to restore the default setting.

dynamic-blacklist ap-max *num*

no dynamic-blacklist ap-max

Parameter Description

Parameter	Description
num	The maximum number of the dynamic blacklist on the AP in the range from 1 to 4096.

Defaults

The default is 2048.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the maximum number of dynamic blacklist members on the AP to 1000.

```
FS(config-wids)# dynamic-blacklist ap-max 1000
```

The following example restores the default setting.

```
FS(config-wids)#no dynamic-blacklist ap-max
```

Platform Description

N/A

2.39 dynamic-blacklist mac-address

Use this command to configure dynamic blacklist entries. Use the **no** form of this command to remove dynamic blacklist entries.

dynamic-blacklist mac-address *H.H.H*

no dynamic-blacklist mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Configures a dynamic blacklist entry.

Defaults

No dynamic blacklist entry is configured by default.

Command Mode

WIDS configuration mode

Usage Guide

Use this command to configure dynamic blacklist entries so as to control STA access and communication policy dynamically.

Configuration Examples

The following example configures MAC 0000.0000.0001 as a dynamic blacklist entry.

```
FS(config-wids)#dynamic-blacklist mac-address 0000.0000.0001
```

The following example removes MAC 0000.0000.0001 from the dynamic blacklist.

```
FS(config-wids)#no dynamic-blacklist mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.40 hybrid-scan radio

Use this command to enable the radio scan. Use the **no** form of this command to disable the radio scan.

hybrid-scan radio *num* **enable**

hybrid-scan radio *num* **disable**

Parameter Description

Parameter	Description
radio *num*	Radio number.

Defaults This function is enabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example disables the scan for radio 1.

```
FS#configure
FS(config)#ap-config ap1
FS(config-ap)#hybrid-scan radio 1 disable
```

Platform Description N/A

2.41 kickout client

Use this command to kick out associate users.

kickout client *H.H.H*

Parameter Description

Parameter	Description
H.H.H	The MAC address of the user to kick out.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide Use this command to disconnect a specified STA association.

Configuration Examples The following example kicks out the MAC address 0000.0000.0001.

```
FS(config-wids)# kickout client 0000.0000.0001
```

Platform Description N/A

2.42 kickout threshold

Use this command to kick out the low-rate STA. Use the **no** form of this command to restore the default setting.

kickout threshold *rate*

no kickout threshold

Parameter

Parameter	Description

Description

rate	Packet sending-receiving rate in the range from 0 to 130 in the unit of Mbps.

Defaults The default is 0, indicating not filtering low-rate STA.

Command Mode WIDS configuration mode

Usage Guide This command is used to filter the low-rate STA. When the wireless access end detects that the sending-receiving rate of STA is less than the configured threshold, it disconnects the association.

Configuration Examples The following example filters the STA with sending-receiving rate less than 20 Mbps.

```
FS(config-ac)# kickout threshold 20
```

The following example disables the filtering.

```
FS(config-wids)#no kickout threshold
```

Related Commands

Command	Description
wids	Enters the WIDS configuration mode.

Platform Description N/A

2.43 reset attack-list all

Use this command to clear the entries of all attack lists.

reset attack-list all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all attack lists.

```
FS(config-wids)# reset attack-list all
```

Related

Command	Description

Commands

N/A	N/A

Platform Description

N/A

2.44 reset black-ssid all

Use this command to clear the entries of the SSID blacklist.

reset black-ssid all

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example clears the entries of the SSID blacklist.

```
FS(config-wids)#reset black-ssid all
```

Platform Description

N/A

2.45 reset detected

Use this command to reset the device list detected in a WLAN.

reset detected { **all** | **adhoc** | **rogue** { **ap** | **client** } | **mac-address** *H.H.H* }

Parameter Description

Parameter	Description
all	Indicates you reset all devices detected in a WLAN.
adhoc	Indicates you reset the detected adhoc client.
rogue ap	Indicates you reset the detected Rogue AP.
rogue client	Indicates you reset the detected Rogue client.
mac-address *H.H.H*	Indicates you reset the device with the source MAC address H.H.H.

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide N/A

Configuration Examples

The following example resets the Rogue AP detected in a WLAN.

```
FS(config-wids)# reset detected rogue ap
```

The following example resets the information of detected Rogue APs.

```
FS(config-wids)#reset detected rogue ap
```

The following example resets the information of detected device with MAC address 0000.0000.0001.

```
FS(config-wids)#reset detected mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.46 reset dos-detected

Use this command to clear the information from DOS attack detection according to *CMCC WLAN AC-AP Interoperability Specification*.

reset dos-detected

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples

The following example clears the information from DOS attack detection according to *CMCC WLAN AC-AP Interoperability Specification*.

```
FS(config-wids)#reset dos-detected
```

Platform N/A

Description

2.47 reset dynamic-blacklist

Use this command to reset dynamic blacklist entries.

reset dynamic-blacklist { **all** | **mac-address** *H.H.H* }

Parameter Description

Parameter	Description
all	Indicates you reset all dynamic blacklist entries.
mac-address *H.H.H*	Indicates you reset the dynamic blacklist entry with the source MAC address H.H.H.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples

The following example resets the dynamic blacklist entry with the source MAC address 0000.0000.0001.

```
FS(config)# wids
FS(config-wids)# reset dynamic-blacklist mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.48 reset permit-mac all

Use this command to clear the entries of all permissible MAC address lists.

reset permit-mac all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples

The following example clears the entries of all permissible MAC address lists.

```
FS(config-wids)# reset permit-mac all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.49 reset permit-ssid all

Use this command to clear the entries of all permissible SSID lists.

reset permit-ssid all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples

The following example clears the entries of all permissible SSID lists.

```
FS(config-wids)# reset permit-ssid all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.50 reset permit-vendor all

Use this command to clear the entries of all permissible vendor lists.

reset permit-vendor all

Parameter

Parameter	Description

Description

N/A	N/A

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example clears the entries of all permissible vendor lists.

```
FS(config-wids)# reset permit-vendor all
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.51 reset rogue-ap detected

Use this command to clear the information from Rogue AP detection according to *CMCC WLAN AC-AP Interoperability Specification*.

reset rogue-ap detected

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example clears the information from Rogue AP detection.

```
FS(config-wids)#reset rogue-ap detected
```

Platform Description

N/A

2.52 reset ssid-filter

Use this command to remove all SSIDs or a specified SSID from blacklists and whitelists.

reset ssid-filter { **ssid all** | **in-ssid** *ssid* }

Parameter Description

Parameter	Description
ssid all	All SSIDs.
in-ssid *ssid*	The specified SSID.

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example removes all SSIDs from blacklists and whitelists.

```
FS(config-wids)#reset ssid-filter ssid all
```

Platform Description

N/A

2.53 reset ssid-filter blacklist all

Use this command to remove all SSIDs from blacklists.

reset ssid-filter blacklist all

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example clears all the SSIDs from blacklists,

```
FS(config-wids)#reset ssid-filter blacklist all
```

Platform Description

N/A

2.54 reset ssid-filter blacklist all in-ssid

Use this command to remove a specified SSID from blacklists.

reset ssid-filter blacklist all in-ssid *string*

Parameter Description

Parameter	Description
string	Removes specified SSIDs from the blacklist.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example removes SSID: my-vlan from blacklists.

```
FS(config-wids)#reset ssid-filter blacklist all in-ssid my-wlan
```

Platform Description N/A

2.55 reset ssid-filter whitelist all

Use this command to remove all SSIDs from whitelists.

reset ssid-filter whitelist all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example removes all SSIDs from whitelists.

```
FS(config-wids)#reset ssid-filter whitelist all
```

Platform Description N/A

2.56 reset ssid-filter whitelist all in-ssid

Use this command to remove a specified SSID from whitelists.

reset ssid-filter whitelist all in-ssid *string*

Parameter Description

Parameter	Description
string	Removes all the whitelists from a specified SSID.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example removes SSID: my-wlan from whitelists.

```
FS(config-wids)#reset ssid-filter whitelist all in-ssid my-wlan
```

Platform Description N/A

2.57 reset static-blacklist all

Use this command to clear the entries of all static blacklists.

reset static-blacklist all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all static blacklists.

```
FS(config-wids)# reset static-blacklist all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.58 reset statistic all

Use this command to clear attack detection statistics.

reset statistic all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears attack detection statistics.

```
FS(config-wids)# reset statistic all
```

Platform Description N/A

2.59 reset unknown-sta all

Use this command to clear the entries of unknown STA lists.

reset unknown-sta all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of unknown STA lists.

```
FS(config-wids)#reset unknown-sta all
```

Platform N/A

Description

2.60 reset user-isolation-permit-list all

Use this command to clear the entries of all permissible lists for user isolation.

reset user-isolation-permit-list all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example clears the entries of all permissible lists for user isolation.

```
FS(config-wids)# reset user-isolation-permit-list all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.61 reset whitelist all

Use this command to clear the entries of all whitelists.

reset whitelist all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration The following example clears the entries of all whitelists.

Examples

```
FS(config-wids)# reset whitelist all
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.62 rogue-ap countermeasures enable

Use this command to enable Rogue AP countermeasures according to *CMCC WLAN AC-AP Interoperability Specification*. Use the **no** form of this command to restore the default setting.

rogue-ap countermeasures enable

no rogue-ap countermeasures enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The function is disabled by default.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables Rogue AP countermeasures.

```
FS(config-wids)#rogue-ap countermeasures enable
```

The following example disables Rogue AP countermeasures.

```
FS(config-wids)#no rogue-ap countermeasures enable
```

Platform Description

N/A

2.63 scan-channels { 802.11a | 802.11b } channels

Use this command to configure the scan channel. Use the **no** form of this command to restore the default setting.

scan-channels { **802.11a** | **802.11b** } **channels** *nuim1 num2…num13*

no scan-channels { **802.11a** | **802.11b** }

Parameter Description

Parameter	Description
802.11a	5GHz channel.

802.11b	2.4GHz channel.
channels *num*	Channel value.

Defaults No scan channel is configured by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the 5GHz scan channel as 149 153 157.

```
FS#configure
FS(config)#ap-config ap1
FS(config-ap)#scan-channels 802.11a channels 149 153 157
```

Platform Description N/A

2.64 show wids attacklist

Use this command to display the WIDS static attack list.

show wids attack-list

Parameter Description

Parameter	**Description**
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the WIDS static attack list.

```
FS# show wids attack-list
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

2.65 show wids blacklist

Use this command to display the static or dynamic blacklist.

show wids blacklist { **static** | **dynamic** }

Parameter Description

Parameter	Description
static	Displays the static blacklist.
dynamic	Displays the dynamic blacklist.

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples

The following example displays the static blacklist.

```
FS# show wids blacklist static
```

The following example displays the dynamic blacklist.

```
FS# show wids blacklist dynamic
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.66 show wids black-ssid

Use this command to display the SSID blacklist.

show wids black-ssid

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the SSID blacklist.

```
FS# show wids black-ssid
```

Platform Description

N/A

2.67 show wids detected

Use this command to display the devices detected in a WLAN.

show wids detected { **adhoc** | **all** | **friendly ap** | **interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }

Parameter Description

Parameter	Description
adhoc	Displays the detected ad-hoc network.
all	Displays all devices detected in a WLAN.
friendly ap	Displays the detected friendly AP.
interfering ap	Displays the detected interference AP.
rogue adhoc-ap	Displays the detected Rogue ad-hoc AP.
rogue ap	Displays the detected Rogue AP.
rogue client	Displays the detected Rogue Client.
rogue config-ap	Displays the detected Rogue config AP.
rogue ssid -ap	Displays the detected Rogue SSID AP.
mac-address *H.H.H*	Displays the detected device with the source MAC address H.H.H.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the Rogue AP detected in a WLAN.

```
FS# show wids detected rogue ap
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.68 show wids dos-detected

Use this command to display the information from DOS detection according to *CMCC WLAN AC-AP Interoperability*

Specification.

show wids dos-detected

Parameter Description

Parameter	**Description**
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the information from DOS detection according to *CMCC WLAN AC-AP Interoperability Specification*.

```
FS# show wids dos-detected
```

Platform Description

N/A

2.69 show wids ssid-filter

Use this command to display the blacklists and whitelists for all SSIDs or a specified SSID.

show wids ssid-filter { **blacklist all** [**in-ssid** *string*] | **ssid all** | **whitelist all** [**in-ssid** *string*] }

Parameter Description

Parameter	**Description**
blacklist all	Displays the blacklists for all SSIDs.
blacklist all in-ssid *string*	Displays the blacklists for a specified SSID.
ssid all	Displays the blacklists and whitelists for all SSIDs.
white all	Displays the whitelists for all SSIDs.
whitelist all in-ssid *string*	Displays the whitelists for a specified SSID.

Defaults

N/A

Command Mode

Privileged EXEC mode.

Usage Guide

N/A

Configuration Examples

The following example displays the blacklists for all SSIDs.

```
FS# show wids ssid-filter blacklist all
```

Related Commands

Command	**Description**

N/A	N/A

Platform Description N/A

2.70 show wids permitted

Use this command to display the MAC address, SSID, and vendor lists trusted in a WLAN.

show wids permitted { **mac-address** | **ssid** | **vendor** }

Parameter Description

Parameter	Description
mac-address	Displays the trusted MAC address list.
ssid	Displays the trusted SSID list.
vendor	Displays the trusted vendor list.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the SSID list trusted in WLAN.

```
FS# show wids permitted ssid
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.71 show wids rogue-ap detected

Use this command to display the information from Rogue AP detection according to *CMCC WLAN AC-AP Interoperability Specification*.

show wids rogue-ap detected

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information from Rogue AP detection according to *CMCC WLAN AC-AP Interoperability Specification*.

```
FS# show wids rogue-ap detected
```

Platform Description N/A

2.72 show wids statistics

Use this command to display the IDS attack detection statistics.

show wids statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the IDS attack detection statistics.

```
FS# show wids statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.73 show wids unknown-sta

Use this command to display the entries of unknown STA lists.

show wids unknown-sta

Parameter Description

Parameter	Description
N/A	N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the entries of unknown STA lists.

```
FS# show wids unknown-sta
```

Platform Description N/A

2.74 show wids user-isolation permit-mac

Use this command to display the information of the permissible MAC address list for user isolation.

show wids user-isolation permit-mac

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information of the permissible MAC address list for user isolation.

```
FS# show wids user-isolation permit-mac
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.75 show wids whitelist

Use this command to display the whitelist.

show wids whitelist

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the whitelist.

```
FS# show wids whitelist
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.76 ssid-filter max

Use this command to configure the maximum number of the blacklist and whitelist members for SSIDs. Use the **no** form of this command to restore the default setting.

ssid-filter max *num*

no ssid-filter max

Parameter Description

Parameter	Description
num	The maximum number of the blacklist and whitelist members in the range from 1 to 128.

Defaults The default is 64.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum number of the blacklist and whitelist members for SSIDs as 40.

```
FS(config-wids)# ssid-filter max 40
```

The following example restores the default setting.

```
FS(config-wids)#no ssid-filter max
```

Platform N/A

Description

2.77 ssid-filter blacklist mac-address in-ssid

Use this command to configure an entry for a specified SSID blacklist. Use the **no** form of this command to restore the default setting.

ssid-filter blacklist mac-address *H.H.H* **in-ssid** *string*

no ssid-filter blacklist mac-address *H.H.H* **in-ssid** *string*

Parameter Description

Parameter	Description
H.H.H	The MAC address of an entry to configure.
string	SSID.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This command is not allowed to use when there is the same entry in the SSID whitelist.

Configuration Examples

The following example configures MAC 0000.0000.0001 for the blacklist of SSID: my-wlan.

```
FS(config-wids)# ssid-filter blacklist mac-address 0000.0000.0001 in-ssid my-wlan
```

The following example restores the default setting.

```
FS(config-wids)# no ssid-filter blacklist mac-address 0000.0000.0001 in-ssid my-wlan
```

Platform Description N/A

2.78 ssid-filter blacklist max

Use this command to set the maximum number of the SSID blacklist members. Use the **no** form of this command to restore the default setting.

ssid-filter blacklist max *num*

no ssid-filter blacklist max

Parameter Description

Parameter	Description
num	The maximum number of the SSID blacklist members in the range from 1 to 256.

Defaults The default is 256.

Command WIDS configuration mode

Mode

Usage Guide N/A

Configuration Examples

The following example sets the maximum number of the blacklist members as 50.

```
FS(config-wids)#ssid-filter blacklist max 50
```

The following example restores the default setting.

```
FS(config-wids)#no sid-filter blacklist max
```

Platform Description N/A

2.79 ssid-filter whitelist mac-address in-ssid

Use this command to configure an entry for a specified SSID whitelist. Use the **no** form of this command to restore the default setting.

ssid-filter whitelist mac-address *H.H.H* **in-ssid** *string*

no ssid-filter whitelist mac-address *H.H.H* **in-ssid** *string*

Parameter Description

Parameter	Description
H.H.H	The MAC address of the entry configured for the specified SSID whitelist.
string	The specified SSID.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide This command is not allowed to use when there is the same entry in the SSID blacklist.

Configuration Examples

The following example configures MAC 0000.0000.0001 to the whitelist of SSID: my-wlan.

```
FS(config-wids)# ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

The following example restores the default setting.

```
FS(config-wids)# no ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

Platform Description N/A

2.80 ssid-filter whitelist max

Use this command to set the maximum number of the SSID whitelist members. Use the **no** form of this command to restore the default setting.

ssid-filter whitelist max *num*

no ssid-filter whitelist max

Parameter Description

Parameter	Description
num	The maximum number of the SSID whitelist members in the range from 1 to 256.

Defaults

The default is 256

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the maximum number of the whitelist members as 50.

```
FS(config-wids)#ssid-filter whitelist max 50
```

The following example restores the default setting.

```
FS(config-wids)#no sid-filter whitelist max
```

Platform Description

N/A

2.81 static-blacklist mac-address

Use this command to configure an entry for the static blacklist. Use the **no** form of this command to delete the static blacklist

static-blacklist mac-address *H.H.H*

no static-blacklist mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates you set the device with the source MAC address H.H.H as a static blacklist entry.
no	Indicates you delete the static blacklist.

Defaults

N/A

Command Mode

WIDS configuration mode

Usage Guide

This command is not allowed if the MAC address exists in the whitelist.

Configuration Examples

The following example configures the device with the source MAC address 0000.0000.0001 to the static blacklist.

```
FS(config-wids)# static-blacklist mac-address 0000.0000.0001
```

The following example restores the default setting.

```
FS(config-wids)# no static-blacklist mac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.82 static-blacklist max

Use this command to configure the maximum number of static blacklist members.

Use the **no** form of this command to restore the default setting.

static-blacklist max *number*

no static-blacklist max

Parameter Description

Parameter	Description
number	Specifies the maximum number of static blacklist members in the range from 1 to 2048.

Defaults

The default is 1024.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the maximum number of static blacklist members to 1000.

```
FS(config-wids)# static-blacklist max 1000
```

The following example restores the default setting.

```
FS(config-wids)#no static-blacklist max
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.83 user-isolation enable

Use this command to enable user isolation on the AP or AC. Use the **no** form of this command to disable this function.

user-isolation { **ap** | **ssid-ap** | **wlan-id** *num* } **enable**

no user-isolation { **ap** | **ssid-ap** | **wlan-id** *num* } **enable**

Parameter Description

Parameter	Description
ap	Enables user isolation on the AP.
ssid-ap	Enables SSID-based user isolation on the AP.
wlan-id *num*	Enables WLAN based user isolation on the AP according to *CMCC WLAN AC-AP Interoperability Specification*.

Defaults This function is disabled by default.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples N/A

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.84 user-isolation permit-mac mac

Use this command to configure a permissible MAC address list for user isolation. Use the **no** form of this command to delete a permissible MAC address.

user-isolation permit-mac mac *H.H.H*

no user-isolation permit-mac mac *H.H.H*

Parameter Description

Parameter	Description
H.H.H	The permissible MAC address list for user isolation.

Defaults N/A

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets MAC 0000.0000.0001 as a permissible MAC for user isolation.

```
FS(config-wids)# user-isolation permit-mac mac-list 0000.0000.0001
```

The following example deletes MAC 0000.0000.0001 from the permissible MAC address list.

```
FS(config-wids)#no user-isolation permit-mac 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.85 user-isolation permit-mac max

Use this command to configure the maximum number of a permissible MAC address list for user isolation.

Use the **no** form of this command to restore the default setting.

user-isolation permit-mac max *num*

no user-isolation permit-mac max

Parameter Description

Parameter	Description
num	The maximum number of a permissible MAC address list for user isolation in the range from 1 to 2048.

Defaults

The default is 1024.

Command Mode

WIDS configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the maximum number of a permissible MAC address list for user isolation to 100.

```
FS(config-wids)# user-isolation permit-mac max 100
```

The following example restores the default setting.

```
FS(config-wids)#no user-isolation permit-mac max
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

2.86 whitelist mac-address

Use this command to configure an entry for the whitelist. Use the **no** form of this command to delete the whitelist

whitelist mac-address *H.H.H*

no whitelist mac-address *H.H.H*

Parameter Description

Parameter	Description
H.H.H	Indicates you set the device with the source MAC address H.H.H as a whitelist entry.

Defaults N/A

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example configures the device with the source MAC address 0000.0000.0001 to the whitelist.

```
FS(config-wids)# whitelist mac-address 0000.0000.0001
```

The following example deletes the device with the source MAC address 0000.0000.0001 from the whitelist.

```
FS(config-wids)# no whitelistmac-address 0000.0000.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.87 whitelist max

Use this command to configure the maximum number of whitelists.

Use the **no** form of this command to restore the default setting.

whitelist max *num*

no whitelist max

Parameter

Parameter	Description

Description

num	Specifies the maximum number of whitelists in the range from 1 to 2048.

Defaults The default is 1024.

Command Mode WIDS configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum number of whitelists to 1000.

```
FS(config-wids)# whitelist max 1000
```

The following example restores the default setting.

```
FS(config-wids)#no whitelist max
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.88 wids

Use this command to enter the WIDS configuration mode.

wids

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enters the WIDS configuration mode.

```
FS(config)# wids
FS(config-wids)#
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

Chapter 15 WLAN Basic Configuration Commands

1 WLAN Basic Configuration Commands

1.1 ac-controller

Use this command to enter the AC configuration mode from the global configuration mode.

ac-controller

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples

The following example enters the AC configuration mode.

```
FS(config)# ac-controller
FS(config-ac)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.2 acctrl-trap

Use this command to control the switch of a specific trap on AC in AC configuration mode. Use the **no** form of this command to restore the default setting.

acctrl-trap [acap-updown-ctrl | acap-joinfail-ctrl | acap-decryeroreport-ctrl | acap-imageupdt-ctrl | acap-timestamp-ctrl | acsta-oper-ctrl]

no acctrl-trap [acap-updown-ctrl | acap-joinfail-ctrl | acap-decryeroreport-ctrl | acap-imageupdt-ctrl | acap-timestamp-ctrl | acsta-oper-ctrl]

Parameter Description

Parameter	Description
acap-updown-ctrl	Controls the forwarding of the trap message about up/down of the CAPWAP tunnel.
acap-joinfail-ctrl	Controls the forwarding of the trap message that AP failed to join AC.
acap-decryeroreport-ctrl	Controls the forwarding of the trap message that the decryption of CAPWAP messages is failed.
acap-imageupdt-ctrl	Controls the forwarding of the trap message about bin file

	updating of AP.
acap-timestamp-ctrl	Controls the forwarding of the trap message about synchronization.
acsta-oper-ctrl	Controls the forwarding of the trap message about login and logout of STA.

Defaults This function is disabled by default.

Command Mode AC configuration mode

Usage Guide The command is used to control the switch of a specified trap on AC.

Configuration Examples The following example enables the forwarding of the trap message about login and logout of STA on AC.

```
FS(config-ac)# acctrl-trap acsta-oper-ctrl
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.3 ac-name

Use this command to configure an AC name for users to identify the AC. Use the **no** form of this command to restore the default setting.

ac-name *ac-name*

no ac-name

Parameter Description

Parameter	Description
ac-name	Indicates an AC name, which can consist of up to 63 characters, excluding any space.

Defaults The default is the last six bits of the MAC address. For example. the default name for the AC with the MAC address 001a.a916.e7b8 is FS_Ac_16e7b8.

Command Mode AC configuration mode

Usage Guide Configure different names for different ACs to make it easy for users to manage.

Configuration Examples The following example sets the AC name to FS-ac.

```
FS(config-ac)# ac-name FS-ac
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.4 ap-auth

Use this command to enable a specified AP with the access authentication function. Use the **no** form of this command to restore the default setting.

ap-auth { **serial** *serial-string* | **password** *password* | **ac-cert** *ac-cert-name* | **ap-cert** *ap-cert-name* }

no ap-auth { **serial** | **password** | **ac-cert** | **ap-cert** }

Parameter Description

Parameter	Description
serial-string	The serial number of the specified AP.
password	The password of the specified AP.
ac-cert-name	The certificate name of the specified AC.
ap-cert-name	The certificate name of the specified AP.

Defaults

This function is disabled by default.

Command Mode

AP configuration mode

Usage Guide

The access authentication only occurs when the AP goes online. If the AP is already online, authentication occurs the next time the AP gets access.

The **ap-auth-serial** command is not supported in **all** modes for every AP has different serial number.

The certificate configured by the **ap-auth ap-cert** command is saved as **cert.crt** uniformly on the AP and the name cannot be changed.

Configuration Examples

The following example sets the serial number for AP1 to 123456.

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# ap-config AP1
FS(config-ap)# ap-auth serial 123456
```

The following example restores the default setting.

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)# ap-config AP1
FS(config-ap)# no ap-auth serial
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.5 ap-auth enable

Use this command to enable a specified AP with the access authentication function. Use the **no** form of this command to restore the default setting.

ap-auth [**serial** | **password** | **certificate**] **enable**

no ap-auth [**serial** | **password** | **certificate**] **enable**

Parameter Description

Parameter	Description
serial	Serial-number-based authentication.
password	Password-based authentication.
certificate	Certificate-based authentication.

Defaults This function is disabled by default.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example enables the AP with the serial-number-based authentication.

```
FS(config)# ac-controller
FS(config-ac)# ap-auth serial enable
```

The following example restores the default setting.

```
FS(config)# ac-controller
FS(config-ac)# no ap-auth serial enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.6 ap-auth serial-update

Use this command to enable all online APs to update their serial numbers.

ap-auth serial-update

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example enables all online APs to update their serial numbers.

```
FS(config)# ac-controller
FS(config-ac)# ap-auth serial-update
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.7 ap-backup group

Use this command to configure an AP backup group in AC configuration mode. Use the **no** form of this command to delete an AP backup group.

ap-backup group *name*

no ap-backup group *name*

Parameter Description

Parameter	Description
name	AP backup group name. “default” is system reserved, namely, “default” cannot be used for backup group configuration.

Defaults By default, the AC device has only one AP backup group named “default”, which takes no effect on the backup function.

Command Mode AC configuration mode

Usage Guide If an AP backup group is deleted, the AP device in this group will be added to the “default” group. The “default” group takes no effect on the backup function.

Configuration Examples The following example configures an AP backup group named apbackup-test-group.

```
FS(config)# ac-controller
FS(config-ac)# ap-backup group apbackup-test-group
```

The following example deletes an AP backup group named apbackup-test-group.

```
FS(config)# ac-controller
FS(config-ac)# no ap-backup group apbackup-test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.8 ap-backup group

Use this command to configure an AP backup group in AP configuration mode. Use the **no** form of this command to remove an AP device from the AP backup group or disable its master AP role.

ap-backup-group *name* [**master**]

no ap-backup-group [*name*] [**master**]

Parameter Description

Parameter	Description
name	AP backup group name
master	(Optional) Designates the AP device as a master AP in the backup group.

Defaults By default, the “default” backup group does not have any AP.

Command Mode AP configuration mode

Usage Guide The backup group must exist before you add an AP device into it.

The **master** parameter designates the AP device as a master AP in the backup group. There is only one master AP in a backup group. If you want to designate a new master AP, use the **no** form of this command to disable the old master AP.

Configuration Examples The following example adds an AP into backup group “backup-test-group” and designates it as a master AP.

```
FS(config)# ap-config AP0001
FS(config-ap)# ap-backup-group backup-test-group master
```

The following example disables a master AP in the backup group.

```
FS(config)# ap-config AP0001
FS(config-ap)# no ap-backup-group backup-test-group master
```

The following example removes an AP from the backup group.

```
FS(config)# ap-config AP0001
FS(config-ap)# no ap-backup-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.9 ap-config

Use this command to enter the configuration mode of a specified AP, which must have been added into an AC. Use the **no** form of this command to restore the default setting.

ap-config *ap-name*

no ap-config *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be configured.

Defaults N/A

Command Mode Global configuration mode

Usage Guide

To enter the configuration mode of a specified AP, ensure this AP must have been added into an AC. The **ap-config all** command can be used to enter the configuration mode of all APs, and the configuration in this mode will be applicable to all APs associated with the AC. The **ap-config** *ap-name* command prevails over the **ap-config all** command.

The **no ap-config** *ap-name* command is used to remove the specified AP configuration. If the target AP is online, it will go offline and then online upon configuration change,

Configuration Examples

The following example configures the AP that has been added with a name AP0001.

```
FS(config-ap)# ap-config AP0001
```

The following example configures the AP that has been offline with a name AP0001.

```
FS(config-ap)# no ap-config AP0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.10 ap-group(AP Configuration Mode)

Use this command to add the AP to a specified AP group. Use the **no** form of this command to restore the default setting.

ap-group *ap-group-name*

no ap-group

Parameter Description

Parameter	Description
ap-group-name	AP group name.

Defaults

The AP joins in the default group by default.

Command Mode

AP configuration mode

Usage Guide

When the AP group is deleted, the member APs of this group are switched to the default group.

Configuration Examples

The following example adds the AP to test-group.

```
FS(config)# ap-group test-group
FS(config-ap-group)#
FS(config)# ap-config AP0001
FS(config-ap)# ap-group test-group
```

The following example restores the default setting.

```
FS(config)# ap-config AP0001
FS(config-ap)# no ap-group test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.11 ap-group

All APs added into an AC always belong to one and only one specific AP group in a certain moment. Any newly added AP belongs to the default AP group: **default**. Use this command to create a new AP group or enter the configuration mode of an existing AP group. If you use this command to create an AP group, you will enter the configuration mode of this AP group once created. Use the **no** form of this command to restore the default setting.

[no] ap-group *ap-group-name*

Parameter

Parameter	Description

Description

ap-group-name	Indicates an AP group name, which consists of up to 150 characters or 64 bytes, excluding any space.

Defaults

By default, the system, once started, will create automatically a default AP group (called **default**), which cannot be created or deleted manually.

Command Mode

AP configuration mode.

Usage Guide

N/A

Configuration Examples

The following example creates an AP group named ***test-group.***

```
FS(config)# ap-group test-group
FS(config-ap-group)#
```

The following example deletes an AP group named ***test-group***.

```
FS(config)#no ap-group test-group
```

The following example enters an AP group named **default**.

```
FS(config)# ap-group default
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.12 ap-mac

Use this command to configure MAC-address-binding. Use the **no** form of this command to remove the configuration.

ap-mac *ap-mac*

no ap-mac

Parameter Description

Parameter	Description
ap-mac	MAC address of the AP.

Defaults

N/A

Command Mode

AP configuration mode

Usage Guide

- With this command configured, the AP configuration takes affect only on the AP whose MAC address is bound.
- In general, MAC-address-binding has a higher priority over name-binding. As long as the AP MAC address is consistent with the preset bound MAC address, the AP adopts the configuration after it goes online.

- Automatic MAC-address-binding: If the specified AP is not configured with MAC-address-binding, when it goes online, the MAC address is bound automatically. The binding is still effective when the AP goes offline.
- MAC-address-binding is also used for AP access control. See the **bind-ap-mac** command for details.
- MAC-address-binding can be performed only on the offline AP.
- In hot backup environment, binding MAC address ensures the consistency of configuration on two ACs.

Configuration Examples

The following example sets the MAC address bound with ap test to 00ff.ffff.1111.

```
FS(config)# ap-config test
FS(config-ap)# ap-mac 00ff.ffff.1111
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.13 ap-name

Use this command to configure the AP name. Use the **no** form of this command to remove the configuration.

ap-name *ap-name*

no ap-name

Parameter Description

Parameter	Description
ap-name	AP name, containing up to 63 characters without blank space.

Defaults

N/A

Command Mode

AP configuration mode

Usage Guide

If the specified AP is online, the AP name configuration takes effect immediately. The name of the AP configuration mode (the string after **ap-config**) is replaced by the new name.

If the specified AP is offline, the AP name configuration takes effect when it goes online. The name of the AP configuration mode does not change until the AP goes online.

After configuring the AP name, you don’t need to exit AP configuration mode before continuing configuration.

If the specified AP is online, the **no** form of this command is not supported

If the specified AP is offline, the **no** form of this command is used to remove the configuration.

If the new name is in use, the configuration fails.

The AP name contains up to 63 characters without blank space.

The AP name cannot be set to **all** or **AP**.

Don’t configure the same name for multiple offline APs. If multiple different offline APs are configured with the same name, the first online AP adopts the new name while the other APs keep the old names.

Configuration Examples

The following example sets the AP0001 name to AP_NEW on an AC.

```
FS(config)# ap-config AP0001
FS(config-ap)# ap-name AP_NEW
```

The following example sets the AP name to AP_TEST.

```
FS(config)# ap-name AP_ TEST
```

Related Commands

Command	Description
N/A	N/A

Platform Description

The command is supported on ACs and fit APs.

1.14 ap-priority

Use this command to enable or disable the support for the Failover priority of APs on an AC.

ap-priority { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables the support for the Failover priority of APs
disable	Disables the support for the Failover priority of APs

Defaults

This function is disabled by default.

Command Mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example establishes a connection between AP0001 and AC1. Configure the priority of AP0001 to 3, and enable the support for the Failover priority of AC1.

```
FS(config)# ap-config AP0001
FS(config-ap)# priority 3
FS(config-ap)# exit
FS(config)# ac-controller
FS(config-ac)# ap-priority enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.15 bind-ap-mac

Use this command to enable AP validity check. Use the **no** form of this command to restore the default setting.

bind-ap-mac

no bind-ap-mac

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode AC configuration mode

Usage Guide When the AP validity check is enabled, only the AP with offline configurations that binds the MAC address can associate the AC. You can configure the command **ap-mac** to binds the MAC address to the offline AP in the AP configuration mode.

Configuration Examples

The following example enables AP validity check.

```
FS(config)# ac-controller
FS(config-ac)# bind-ap-mac
```

The following example disables AP validity check.

```
FS(config)# ac-controller
FS(config-ac)# no bind-ap-mac
```

Related Commands

Command	Description
ap-mac	Binds the MAC address to the offline AP.

Platform Description

1.16 credential

Use this command to configure a username and a password for an AP. Use the **no** form of this command to restore the default setting.

[no] credential *user-name password*

Parameter Description

Parameter	Description
user-name	Indicates a username to be used on an AP, which can consist of up to 255 characters, excluding any space.
password	Indicates a password to be set on an AP, which can consist of up to 255 characters, excluding any space.

Defaults N/A

Command Mode AP configuration mode or AP group configuration mode

Usage Guide N/A

Configuration Examples

The following example configures a username **first-ap** and a password **123456** for AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# credential first-ap 123456
```

The following example configures a username **first-ap** and a password **123456** for all APs in the AP group (default).

```
FS(config)# ap-group default
FS(config-ap-group)# credential first-ap 123456
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.17 enable-broad-ssid

Use this command to enable SSID broadcast in the WLAN configuration mode. Use Tthe **no** form of this command to disable this function.

[no] enable-broad-ssid

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode WLAN configuration mode

Usage Guide When you configure the Suppress SSID information of this WLAN, the configuration will take effect only if completed before the WLAN is applied.

Configuration Examples

The following example enables SSID broadcast on this WLAN.

```
FS(config-wlan)#enable-broad-ssid
```

The following example disables SSID broadcast on this WLAN.

```
FS(config-wlan)#no enable-broad-ssid
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.18 factory-reset

Use this command to restore the factory setting of a specified AP, that is, to reset this AP.

factory-reset *ap-name*

Parameter Description

Parameter	Description
ap-name	indicates the name of the AP that needs to restore factory setting.

Defaults N/A

Command Mode AC configuration mode

Usage Guide The configuration will restore the factory setting of a specified AP, and as a result, the operation will reset this AP.

Configuration Examples The following example configures AP0001 to restore its factory setting.

```
FS(config-ac)# factory-reset AP0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.19 interface-mapping

Use **interface-mapping** in AP group configuration mode to map **wlan-vlan** or **wlan-vlan-group mapping** (the mapping in all descriptions of this cli refers to map wlan-vlan or wlan-vlan-group mapping) to the radios of all the APs in an AP group. The related WLAN configuration can be applied to the specified radio through such mapping. Use the **no** form this command to remove the related mapping configuration.

interface-mapping *wlan-id* [*vlan-id* I **group** *vlan-group-id*] [**radio** {*radio-id* | [*802.11b* | *802.11a*]}] [**ap-wlan-id** *ap-wlan-id*]

no interface-mapping *wlan-id* [*vlan-id* I **group** *vlan-group-id*] [**radio** {*radio-id* | [*802.11b* | *802.11a*]}] [**ap-wlan-id** *ap-wlan-id*]

Parameter Description

Parameter	Description
wlan-id	ID of the WLAN to be mapped. This WLAN must be created already. Its ID ranges from 1 to 4094.
vlan-id	ID of the VLAN to be mapped. This VLAN must be created already.

	Its ID ranges from 1 to 4094.
vlan-group-id	ID of the VLAN-group to be mapped. This VLAN-group must be created already. Its ID ranges from 1 to 128.
radio-id	An AP's radio to which the specified mapping is applied. Its reserved range is the standard, defined 1 to 48. Currently, the product should use the range of 1 to 2. If no radio-id is specified, the mapping will be applied to all the radios of all the APs in the AP group.
802.11b	Applies the mapping to 2.4G radio.
802.11a	Applies the mapping to 5.8G radio.
ap-wlan-id	Specifies the WLAN ID on the AP, in the range from 1 to 64. If the WLAN ID is not specified, the mapping selects an available ID automatically.

Defaults

N/A

Command Mode

AP group configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures VLAN 2 and a WLAN with its ID of 4094, and apply the mapping of wlan4094-vlan2 to radio 1 of all the APs in the default AP group.

```
FS(config)#vlan 2
FS(config)#wlan-config 4094 pro-4094 ssid-4094
FS(config-wlan)#exit
FS(config)#ap-group default
FS(config-ap-group)#interface-mapping 4094 2 radio 1
```

The following example configures VLAN-group 3 and a WLAN with its ID of 4094, and apply the mapping of wlan4094-vlan-group3 to all the radios of all the APs in the default AP group.

```
FS(config)#vlan-group 3
FS(config)#wlan-config 4094 pro-4094 ssid-4094
FS(config-wlan)#exit
FS(config)#ap-group default
FS(config-ap-group)#interface-mapping 4094 group 3
```

The following example configures the default AP group and delete the configured wlan4094-vlan2 mapping.

```
FS(config)# ap-group default
FS(config-ap-group)# no interface-mapping 4094 2 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.20 logging on

Use this command globally to allow logs to be displayed on different devices. Use the **no** form of this command to disable this fucntion.

logging on

no logging on

Parameter Description

Parameter	Description
N/A	N/A

Defaults Logs are allowed to be displayed on different devices by default.

Command Mode AP configuration mode

Usage Guide

Configuration Examples The following example disables the log display on the device.

```
FS(config)# no logging on
```

Related Commands

Command	Description
logging buffered	Records the logs to a memory buffer.
logging	Sends logs to the Syslog server.
logging file flash:	Records logs on the extended FLASH.
logging console	Allows the log level to be displayed on the console.
logging monitor	Allows the log level to be displayed on the VTY window (such as telnet window) .
logging trap	Sets the log level to be sent to the Syslog server.

Platform Description

1.21 logging server

Use this command to record the logs in the specified Syslog Sever. Use the **no** form of the command to restore the default setting.

logging server *ip-address* [**udp-port** *num*]

no logging server *ip-address*

Parameter Description

Parameter	Description

ip-address	IP address of the host that receives log information.
num	Port number of the host that receives log information.

Defaults N/A

Command Mode AP configuration mode/All APs configuration mode

Usage Guide This command specifies a Syslog server to receive the logs of the device. Users are allowed to configure up to 5 Syslog servers. The log information will be sent to all the configured Syslog servers at the same time.

Configuration Examples The following example specifies a syslog server of the address 202.101.11.1:

```
FS(config)# logging server 202.101.11.1
```

Related Commands

Command	Description
logging on	Turns on the log switch.
show logging	Views log messages and related log configuration parameters in the buffer.
logging trap	Sets the level of logs allowed to be sent to Syslog server.

Platform Description

1.22 nas-id

Use this command to set the access ID for the WLAN user or AC. Use the **no** form of this command to restore the default setting.

nas-id *nas-id*

no nas-id

Parameter Description

Parameter	Description
nas-id	Access ID, containing 32 characters without blank space.

Defaults The default WLAN user access ID is an empty string.

The default AC access ID is the AC MAC address in dotted format.

Command Mode WLAN configuration mode/AC configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the access ID for the WLAN user to 0000059159100460.

```
FS(config)#show wlan-config cb 1
WLAN ID................................. 1
SSID.................................... 1-leichen-test-wlan
Profile.................................
MAC Mode................................ Local
Tunnel Mode............................. 802.3 Tunnel
Suppress SSID........................... Disable
Sta-limit............................... 0
NAS ID.................................. 0000059159100460
Band Select............................. Disable
SSID Code...............................
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.23 priority

Use this command to set the Failover priority of APs. After you enable the support for the Failover priority of APs on an AC, the AC can accept the access of APs according to their priority order.

priority *priority-value*

Parameter Description

Parameter	Description
priority-value	The parameter indicates the Failover priority of APs. The allowed value is 1, 2, 3, and 4.

Defaults

The default is 1.

Command Mode

AP configuration mode

Usage Guide

Configure the Failover priority of devices. **1** indicates the lowest priority, and **4** indicate the highest priority. Add the AC sequence (priority of APs) to the AP. The configurations are saved in the AP. When the AP is associated next time, the configurations take effect.

Configuration

The following example sets the Failover priority of the AP group named **apgroup** to 3.

Examples

```
FS#config terminal
FS(config)#ap-config apgroup
FS(config-ap)#priority 3
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.24 reload at

Use this command to enable AP restart as scheduled every day. Use the **no** form of this command to remove the configuration.

reload at *time*

no reload at

Parameter Description

Parameter	Description
time	AP restart time every day, in the format of hh:mm:ss.

Defaults N/A

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example enables AP restart at 1:00:00 every day.

```
FS(config)#ap-config FS-AP1
FS(config-ap)#reload at 1:00:00
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.25 reset

In the AC configuration mode, use this command to reset all APs, reset any AP with an updated software version, and reset any specified AP.

reset{all | |single *ap-name*}

Parameter Description

Parameter	Description
all	Indicates that all APs will be reset.
single *ap-name*	Indicates that a specified AP will be reset.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example resets all APs.

```
FS(config-ac)# reset all
```

The following example resets the AP named AP0001.

```
FS(config-ac)# reset AP0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.26 sshow ac-config

Use this command to display the basic configuration information about the current AC.

show ac-config

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the basic configuration information of the current AC.

```
FS(config)#show ac-config
AC Configuration info:
max_wtp                :128
sta_limit              :4096
license wtp max    :128
license sta max    :4096
serial auth           :Disable
```

```
password auth        :Disable
certificate auth :Disable
Bind AP MAC           :Disable
AP Priority           :Disable
ac_name                   :FS_Ac_231455
ac location           :FS_COM

AC State info:
sta_num                   :0
act_wtp                  :12
used wtp              :8( 4 normal 8 half)
remain wtp              :120 normal 240 half
HW Ver                    :1.0
SW Ver                    :AC_FSOS 11.1(1)B1
Mac address          :001a.9923.1455
Product ID             :WS5708
NET ID                   :9876543210012345
NAS ID                   :001a.9923.1455
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.27 show ac-config ap-backup-group

Use this command to display the AP backup group.

show ac-config ap-backup-group [*group-name*]

Parameter Description

Parameter	Description
group-name	AP backup group name. The "default" group is not displayed.

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the all AP backup groups.

```
FS#show ac-config ap-backup-group
Cnt      Group-Name                          Master-AP cnt     Standby-AP cnt       Master-AP-Name        Working
------ ---------------------------------- ------------ ----------- ------------     -----------
```

```
1         AP-BACKUP-GROUP1              1                  2                        AP4210-1                false
```

The following example displays details of backup group “AP-BACKUP-GROUP1”.

```
FS#show ac-config ap-backup-group AP-BACKUP-GROUP1
Cnt        Ap-Name                              Ap-Mac                  Online      Is-Master     Inherit-Wlan Cnt
------- ------------------------ -------------------- ------- ------------ -----------------
1         AP4210-1                           8832.0000.1111          true          Yes            0
2         APD-M-1                                    -                    false         No             0
3         APD-M-2                            0011.4477.8833          true          No             0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.28 show ap-config bssid

Use this command to display the BSSID list.

show ap-config bssid

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the BSSID list.

```
FS(config)#show ap-config bssid
AP Mac               Radio ID WLAN ID    BSSID
-------------- -------- -------- --------------
5869.6c75.7677              1              2 0669.6c75.7679
5869.6c75.7677              2              2 0669.6c75.767a
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.29 show ap-config cb

Use this command to display the status information of an AP.

show ap-config cb *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the status information of an AP.

```
ac#show ap-config cb wlan-ap-0001
Configuration:
ap name                       :wlan-ap-0001
ap id                         :1
discovery timer               :20
echo request timer            :30
error report timer            :120
client timeout timer          :300
statistisc time               :120
ap fallback                   :1
image id                      :FSOS 10.4 (1t7)(1T7), Release(73413)
group name                    :default
dhcp_option                   :standard
Core dump server ip           :0.0.0.0
Core dump file name           :

Status:
local ipv4                    :192.168.120.2
Tran protocol                 :udp
Discovery type                :unknow
ECN Support                   :0
location data                 :Not Setting
mtu                           :0
session id                    :0x0f075476,0x0f075476,0x0f075476,0x0f075476
tunnel mode                   :0xe(NELR)
mac type                      :full support
WTP Name                      :wlan-ap-0001
STA Limit                     :30
STA num                       :2
```

```
radio num                    :1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.30 show ap-config inherit-wlan

Use this command to display the WLAN inherited by the specified AP device in backup group.

show ap-config inherit-wlan *ap-name*

Parameter Description

Parameter	Description
ap-name	AP name

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the WLAN inherited by the specified AP in the backup group.

```
ac#show ap-config inherit-wlan wlan-ap-0001
WLAN ID    SSID                    VLAN-Id/VLAN-Group ID     Radio ID                  AP WLAN ID
-------- --------------------- ------------------------ ------------------------- ----------
1          FS-wifi              1100                      ALL
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.31 show ap-config product

Use this command to display the AP device list.

show ap-config product

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples

The following example displays the AP device list.

```
FS#show ap-config product
Product ID             Hardware Version Count    Used Wtp
-------------------- ---------------- -------- --------
AP120                              1.0        10        5.0
AP220-E                            1.0         5        5.0
AP320                              2.0         8        8.0
AP530-PPC                          1.5         2        2.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.32 show ap-config summary

Use this command to display the AP list.

show ap-config summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the AP list.

```
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
       Channel: * = Global
       Power Level = Percent

Online AP number: 2
```

```
Offline AP number: 1

AP Name                                              IP Address          Mac Address        Radio
Radio                         Up/Off time      State
---------------------------------------- --------------- -------------- ------------------- ------------------- ------------- -----
AP220E-2                                            22.22.22.11         00d0.1414.3f67 1    E      0      11*    100 2    E
0    153*    100        0:00:37:34 Run
xh-ap                                               10.21.121.4         00d0.f822.33d6 1# N      0       -          - 2# N
0        -          -        0:23:56:05 Run
AP220E_V2.0_19                                              -               1414.4b13.96f7 1    N     -       -          - 2    N
-        -          -        0:00:14:07 Quit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.33 show ap-config summary ap-auth

Use this command to display authentication information on all APs.

show ap-config summary ap-auth

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays authentication information on all APs.

```
FS#sh ap-config summary ap-auth
AP Name                                  Mac Address       Bind    bind-ap-serial      Bind    bind-ap-cert
Bind    bind-ap-password Bind    State
-------------------------- -------------- ----- ---------------- ----- ------------------------- ----- ---------------- ----- -----
ap220                                    1414.4b13.9ff3 FALSE                              TRUE
FALSE                              TRUE    Run
0011.0000.0101                                         FALSE                              TRUE
FALSE                              TRUE    Quit
0011.0000.0201                                         FALSE                              TRUE
```

```
FALSE                           TRUE    Quit
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.34 show ap-config summary deny-ap

Use this command to display the list of APs that are refused in attempt to associate with the AC.

show ap-config summary deny-ap

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the list of APs that are refused in attempt to associate with the AC.

```
FS#sh ap-config summary deny-ap
AP Name          IP Address              Mac Address         Reason
-----------     -----------------     -------------- --------------
AP1                  192.168.10.10         1414.4b13.9ff3    By bind-ap-mac
AP2                  192.168.10.11         00d0.f822.33b0    By bind-ap-mac
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.35 show ap-group aps

Use this command to display the list of APs connected to a specified AP group.

show ap-group aps *ap-group-name*

Parameter

Parameter	Description

Description

ap-group-name	Indicates an AP group name.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the basic configuration information of the current AC.

```
FS(config)#show ap-group aps default
Ap Name                  Mac Addr          Pid
-------------------- --------------- --------------------
rrm-ap                 0011.1122.3333 AP220E
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.36 show ap-group aps summary

Use this command to display the APs of all AP groups.

show ap-group aps summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the APs of all AP groups.

```
FS(config)#show ap-group aps summary
AP Group Name           AP Name                    Mac Addr
-------------------- -------------------- ---------------
default                 rrm-ap                    0011.1122.3333
default                 ap0001                     0011.1122.4444
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.37 show ap-group cb

Use this command to display the basic configuration information of a specified AP group.

show ap-group cb *ap-group-name*

Parameter Description

Parameter	Description
ap-group-name	Indicates an AP group name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the basic configuration information of the default AP group.

```
FS(config)#show ap-group cb default

Ap Group info:
apg_name             :default
discovery_timer      :20
echo_req_timer       :30
error_report_timer   :120
sta_time_out         :300
stati_time           :120
ap_fallback          :Enable
image_id             :
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.38 show ap-group intf-wlan-map

Use this command to display the WLAN-to-VLAN mapping table of a specified AP group.

show ap-group intf-wlan-map *ap-group-name*

Parameter Description

Parameter	Description
ap-group-name	Indicates an AP group name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the basic configuration information of the current AC.

```
FS(config)#show ap-group intf-wlan-map default
WlAN ID      SSID                      Vlan Id                  Radio id      Mib index
--------- ---------------- ---------------- ---------- ----------------
500          ssid-500               2                            ALL             1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.39 show ap-group summary

Use this command to display the list of all AP groups configured for the current AC.

show ap-group summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the list of all AP groups configured for the current AC.

```
FS(config)#show ap-group summary
Total Ap Group Num : 2
Ap Group Name
1. default
2. test-group
```

Related

Command	Description

Commands

N/A	N/A

Platform Description

1.40 show wlan-config cb

Use this command to display the configuration details of a specified WLAN.

show wlan-config cb *wlan-id*

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the configuration of WLAN 512.

```
FS(config)#show wlan-config cb    512
WLAN ID................................. 512
SSID.................................... ssid-512
Profile................................. <NULL>
Short Preamble.......................... Disable
Spectrum Management..................... Disable
QoS..................................... Disable
Short Slot Time......................... Disable
APSD.................................... Disable
Delayed Block ACK....................... Disable
Immediate Block ACK..................... Disable
MAC Mode................................ Local
Tunnel Mode............................. 802.3 Tunnel
Suppress SSID........................... Enable
RTS Threshold........................... 2347
Long Retry.............................. 4
Short Retry............................. 7
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.41 show wlan-config summary

Use this command to display the WLAN configuration list on the AC.

show wlan-config summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the WLAN configuration list on the AC.

```
FS(config)#show wlan-config summary
Total Wlan Num : 3
Wlan id    Profile Name                SSID                          STA NUM
-------- -------------------- -------------------- --------
1             pro-1                          ssid-1                        0
2             pro-2                          ssid-2                        0
4095       <NULL>                       ssid-4095                   0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.42 ssid

Use this command to set SSID.

ssid *ssid-string*

Parameter Description

Parameter	Description
ssid-string	SSID character string, consisting of up to 32 characters.

Defaults N/A

Command Mode WLAN configuration mode

Usage Guide If a WLAN is deployed, changing SSID will disconnected the STAs associated with WLAN.

Configuration Examples

The following example changes the SSID of WLAN1 to FS.

```
FS(config)#wlan-config 1
FS(config-wlan)#ssid FS
```

Related Commands

Command	Description
N/A	N/A

Platform Description

1.43 statistics-timer

Use this command to configure statistics timer for a specified AP or all APs in a specified AP group. Use the **no** form of this command to restore the default configuration.

statistics-timer *timer-num*

no statistics-timer

Parameter Description

Parameter	Description
timer-num	Indicates a timer interval to be configured, in the range from 1 to 65535 in the unit of seconds.

Defaults

The default is 120 seconds.

Command Mode

AP configuration mode or AP group configuration mode

Usage Guide

The command is used to set statistics timer for a specified AP. This command prefixed with no can be used to restore the default value.

Configuration Examples

The following example enters the configuration mode of AP0001 to configure its statistics timer to 200 seconds.

```
FS(config)# ap-config AP0001
FS(config-ap)# statistics-timer 200
```

The following example enters the configuration mode of AP0001 to restore the default setting.

```
FS(config)# ap-config AP0001
FS(config-ap)# no statistics-timer
```

The following example enters the default AP group to configure its statistics timer to 200 seconds.

```
FS(config)# ap-group default
FS(config-ap-group)# statistics-timer 200
```

The following example enters the default AP group to restore the default setting.

```
FS(config)# ap-group default
FS(config-ap-group)# no statistics-timer
```

Related

Command	Description

Commands

N/A	N/A

Platform Description

1.44 wlan-config

Use this command create a WLAN and enter the WLAN configuration mode. Use the **no** form of this command to remove the configuration.

wlan-config *wlan-id* [*profile-string*] [*ssid-string*]

no wlan-config *wlan-id*

Parameter Description

Parameter	Description
wlan-id	Indicates an ID for the WLAN to be created, ranging from 1 to 4094.
profile-string	Indicates a descriptor for the WLAN, which can be omitted.
ssid-string	Indicates the SSID character string corresponding to the WLAN.

Defaults

N/A

Command Mode

WLAN configuration mode

Usage Guide

To create a WLAN, you must specify **ssid-string** but can omit **profile-string** as mentioned in the command description. When a WLAN is created, cli will automatically enter the configuration mode of this WLAN.

To enter the configuration mode of a WLAN, you only need to specify the existing ID of this WLAN.

One SSID can correspond to more than one WLAN, but one WLAN cannot be associated with multiple SSIDs at the same time.

Configuration Examples

The following example creates a WLAN with an ID of 2048 and a SSID of **ssid-test**.

```
FS(config)# wlan-config 2048 profile-test ssid-test
FS(config-wlan)# exit
FS(config)#
```

The following example enters the configuration mode of the WLAN with the ID of 2048.

```
FS(config)# wlan-config 2048
FS(config-wlan)# exit
```

Related Commands

Command	Description
interface-mapping wlan-id vlan-id [**radio** *radio-id*]	Applies this WLAN to a specified radio.

Platform Description

1.45 wtp-limit

Use this command to configure the maximum number of AP supported on the AC. Use the **no** form of this command to restore the default setting.

wtp-limit *wtp-num*

no wtp-limit

Parameter Description

Parameter	Description
wtp-num	The parameter indicates the maximum number of AP connected to the AC.

Defaults The default is **16** for WS5302 , and **128** for WS5708.

Command Mode AC configuration mode

Usage Guide

The command is used to configure the maximum number of AP supported on the AC. This number can exceed neither the maximum number supported by the AC nor the maximum number allowed by the license.

⚠ Different model of AP product has the different weight of supported number, for example, two wall APs occupy one of the maximum number. The AC device will calculate the real number of occupied APs according to the weight ratio. This command is used to configure the weight number of APs instead of real number of APs.

Configuration Examples

The following example configures the AC to connect 100 APs at most.

```
FS(config-ac)# wtp-limit 100
```

The following example configures the AC to connect a default maximum of 128 APs.

```
FS(config-ac)# no wtp-limit
```

Related Commands

Command	Description
sta-limit	Configures the maximum number of clients supported by the AC.

Platform Description

2 WLAN STAMP Commands

2.1 ap

Use this command to configure the AP information in the association control zone. Use the **no** form of this command to delete the specified AP from the association control zone.

ap *WORD*

no ap [*WORD*]

Parameter Description

Parameter	Description
WORD	AP name. The name length range is from 1 to 64.

Defaults No AP information in the association control zone is configured by default.

Command mode Association control zone configuration mode

Usage Guide Up to five APs can be configured in an association control zone. The system will prompt an error message if the number of the configured APs exceeds five. In addition, when configuring AP information for an association control zone, we do not require that APs are online.

Configuration Examples The following example configures a set of AP information with MAC address of 00d0.f800.1001 for an association control zone named “Class (1) Grade 1”.

```
FS(config)#control-zone Class (1) Grade 1
FS(config-cznoe)# ap 00d0.f800.1001
```

Related Commands

Command	Description
show control-zone	Displays the association control zone.

Platform Description This command is supported only on ACs.

2.2 assoc-control

Use this command to enable the association control function. Use **no** form of this command to restore the default setting.

assoc-control

no assoc-control

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command mode Global configuration mode

Usage Guide When the association control function is disabled, the association control related commands can still be configured with the ineffective association control function.

Configuration Examples

The following example enables the association control function.

```
FS(config)#assoc-control
```

The following example disables the association control function.

```
FS (config)#no assoc-control
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.3 client-kick

Use this command to delete the MAC address of a specified wireless user.

client-kick *sta-mac*

Parameter Description

Parameter	Description
sta-mac	Indicates the MAC address of a wireless user.

Defaults

N/A

Command Mode

AC configuration mode

Usage Guide

N/A

Configuration Examples

The following example deletes the wireless user with the MAC address aaaa.bbbb.cccc.

```
FS(config)# ac-controller
FS(config-ac)# client-kick aaaaa.bbbbb.ccccc
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.4 control-zone

Use this command to create an association control zone and enter association control zone configuration mode.

Use the **no** form of this command to restore the default setting.

control-zone *czone-name*

no control-zone *czone-name*

Parameter

Parameter	Description

Description

czone-name	Association control zone name. The name length range is 1 to 64.

Defaults N/A

Command mode Global configuration mode

Usage Guide Up to 300 association control zones can be configured on an AC. Only one association control zone is allowed to be configured on a fat AP. The system will prompt an error message if the upper limit is exceeded.

Configuration Examples The following example configures an association control zone named "Class (1) Grade 1".

```
FS(config)#control-zone Class (1) Grade 1
FS(config- czone)#
```

The following example deletes an association control zone named "Class (1) Grade 1".

```
FS(config)# no control-zone Class (1) Grade 1
The operation will clear the control zone configuration, which may cause corresponding STAs offline. Continue?
[no] y
FS(config)#
```

Related Commands

Command	Description
show control-zone summary	Displays the summary of association control zones.

Platform Description This command is supported only on ACs.

2.5 flow-balance-group add

Use this command to add a specified AP to a specified load balancing group.

flow-balance-group add *group-name ap-name*

Parameter Description

Parameter	Description
group-name	Indicates the name of the specified balancing group. Each flow-based load balancing group supports 10 APs at the most.
ap-name	Indicates the AP's name to be added

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples The following example adds ap1 and ap2 to the balancing group named test-group

```
FS(config)# ac-controller
FS(config-ac)# flow-balance-group add test-group ap1
FS(config-ac)# flow-balance-group add test-group ap2
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.6 flow-balance-group base

Use this command to configure the traffic base value for load balancing. Use the **no** form of this command to restore the default setting.

flow-balance-group base *number*

no flow-balance-group base

Parameter Description

Parameter	Description
number	Traffic base value. The range is from 1 to 100.

Defaults

The traffic base value is 10 Mbps by default.

Command Mode

AC configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the traffic base value for load balancing to 50 Mbps

```
FS(config)# ac-controller
FS(config-ac)# flow-balance-group base 50
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.7 flow-balance-group create

Use this command to configure the load-balancing group based on the flow. Use the **no** form of this command to remove the configuration.

flow-balance-group create *group-name*

no-flow-balance-group create *group-name*

Parameter Description

Parameter	Description
group-name	The name of a load balancing group, allows a maximum of 55 characters and excludes space. It supports 80 flow-balancing groups at most.

Defaults

N/A

Command Mode

AC configuration mode

Usage Guide

The **no** option of this command is used to delete configuration of a specific balancing group.

Configuration Examples

The following example creates a load balancing group named test-group.

```
FS(config)# ac-controller
FS(config-ac)# flow-balance-group create test-group
```

The following example deletes the load balancing group named test-group.

```
FS(config)# ac-controller
FS(config-ac)# no flow-balance-group create test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.8 flow-balance-group del

Use this command to delete a specified AP from a specified load balancing group.

flow-balance-group del *group-name ap-name*

Parameter Description

Parameter	Description
group-name	The load balancing group for operation.
ap-name	The name of AP to be deleted from the load balancing group.

Defaults

N/A

Command Mode

AC configuration mode

Usage Guide

N/A

Configuration Examples

The following example deletes ap1 from balancing group named test-group.

```
FS(config)# ac-controller
FS(config-ac)# flow-balance-group del test-group ap1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.9 flow-balance-group enable

Use this command to configure a threshold value for the traffic of associated AP devices to enable load balancing. Use the **no** form of this command to restore the default threshold value.

flow-balance-group enable *group-name number*

no flow-balance-group enable *group-name number*

Parameter Description

Parameter	Description
group-name	The load balancing group for operation.
number	The traffic threshold value. The unit is %. The range is from 0 to 500. “0” indicates load balancing is disabled.

Defaults The default traffic threshold is 5%.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example sets the traffic threshold of load balancing group test-group to 100 Kbps.

```
FS(config)# ac-controller
FS(config-ac)# flow-balance-group enable test-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.10 flow-balance-group flow

Use this command to configure the load threshold of the balancing group. Use the **no** form of this command to remove the configuration.

[no] flow-balance-group flow *group-name ap-name*

Parameter Description

Parameter	Description
group-name	Name of load balancing group for operation.
number	The threshold of the balancing group, the unit is 100 Kbps, the default is 500 Kbps, and the scope is 0-100000 kbps. 0 indicates this balancing group does not enable flow-based load balancing function.

Defaults The default traffic threshold is 5%.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example configures the threshold of balancing group named test-group as 100 Kbps.

```
FS(config)# ac-controller
FS(config-ac)# flow-balance-group flow test-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.11 flow-balance-group radio-flow

Use this command to configure the load balancing group based on the traffic reported by the AP periodically. Use the **no** form of this command to remove the configuration.

flow-balance-group radio-flow *group-name*

no flow-balance-group radio-flow *group-name*

Parameter Description

Parameter	Description
group-name	Load balancing group name.

Defaults By default, the traffic calculated from the CAPWAP data channel on the AC device is used.

Command mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example configures the load balancing group based on the traffic reported by the AP periodically.

```
FS(config)# ac-controller
FS(config-ac)# flow-balance-group radio-flow test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.12 inter-radio-balance flow-balance dual-band

Use this command to configure the enabling threshold and balancing threshold for the traffic balancing between the different radios (2.4G and 5.0G) of AP devices or AP groups. Use the **no** form of this command to restore the default settings.

inter-radio-balance flow-balance dual-band enable-load *en-num* **threshold** *thrs-num*

no inter-radio-balance flow-balance dual-band

Parameter

Parameter	Description

Description

en-num	The enabling threshold value. Load balancing is enabled only when the traffic on the associated radio exceeds the threshold. The unit is 100 Kbps. The range is from 1 to 1000.
thrs-num	The balancing threshold value. The STA will be disassociated with the radio when the traffic difference between the associated radio and lowest load radio. The unit is 100 Kbps. The range is from 1 to 1000.

Defaults By default, the enabling threshold is 1 Mbps and the balancing threshold is 1 Mbps.

Command mode AP /AP group configuration mode

Usage Guide When the load balancing between radios is enabled, if the traffic of associated radio exceeds the enabling threshold and the traffic difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the traffic will be balanced to radio of lower load. This configuration takes effect only when the radio of lowest load is on the different radio to be associated. The **inter-radio-balance flow-balance same-band** takes effect If the two radios are on the same radio.

Configuration Examples

The following example configures the enabling threshold and balancing threshold to 800 Kbps and 800 Kbps respectively for the different radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# inter-radio-balance flow-balance same-band enable-load 8 threshold 8
```

The following example restores the default load balancing settings for different radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# no inter-radio-balance flow-balance dual-band
```

The following example configures the enabling threshold and balancing threshold to 300 Kbps and 500 Kbps respectively for different radios of AP devices in the AP group.

```
FS(config)# ap-group default
FS(config-group)# inter-radio-balance flow-balance dual-band enable-load 3 threshold 5
```

The following example configures the enabling threshold and balancing threshold to 3 Mbps and 3 Mbps respectively for different radios on all AP devices.

```
FS(config)# ap-config all
FS(config-ap)# inter-radio-balance flow-balance dual-band enable-load 30 threshold 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.13 inter-radio-balance flow-balance enable

Use this command to enable load balancing for traffic between different radios (2.4G and 5.0G) on the AP device or AP group. Use the **no** form of this command to disable load balancing between radios on the AP device or AP group.

inter-radio-balance flow-balance enable

no inter-radio-balance flow-balance enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults By default, load balancing between radios is disabled.

Command mode AP /AP group configuration mode

Usage Guide After load balancing between radios is enabled on an AP device, the AC device will make the traffic difference between radios on the AP device not exceed the threshold value.

Configuration Examples

The following example enables load balancing for traffic between radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# inter-radio-balance flow-balance enable
```

The following example disables load balancing for traffic between radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# no inter-radio-balance flow-balance enable
```

The following example enables load balancing for traffic between radios on the AP devices in the default group.

```
FS(config)# ap-group default
FS(config-group)# inter-radio-balance flow-balance enable
```

The following example enables load balancing for traffic between radios on all AP devices.

```
FS(config)# ap-config all
FS(config-ap)# inter-radio-balance flow-balance enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.14 inter-radio-balance flow-balance same-band

Use this command to configure the enabling threshold and balancing threshold for the traffic balancing between the same radios (both 2.4G or 5.0G) of AP devices or AP groups. Use the **no** form of this command to restore the default settings.

inter-radio-balance flow-balance same-band enable-load *en-num* **threshold** *thrs-num*

no inter-radio-balance flow-balance same-band

Parameter Description

Parameter	Description
en-num	The enabling threshold value. Load balancing is enabled only when the traffic on the associated radio exceeds the threshold. The unit is 100 Kbps. The range is from 1 to 1000.
thrs-num	The balancing threshold value. The STA will be disassociated with the radio when the traffic difference between the associated radio and lowest load radio. The unit is 100 Kbps. The range is from 1o to 1000.

Defaults By default, the enabling threshold is 500 Kbps and the balancing threshold is 500 Kbps.

Command mode AP /AP group configuration mode

Usage Guide When the load balancing between radios is enabled, if the traffic of associated radio exceeds the enabling threshold and the traffic difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the traffic will be balanced to the radio of lower load. This configuration takes effect only when the radio of lowest load is on the different the radio to be associated. The **inter-radio-balance flow-balance dual-band** takes effect If the two radios are on the different radio.

Configuration Examples

The following example configures the enabling threshold and balancing threshold to 800 Kbps and 800 Kbps respectively for the same radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# inter-radio-balance flow-balance same-band enable-load 8 threshold 8
```

The following example restores the default load balancing settings for the same radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# no inter-radio-balance flow-balance same-band
```

The following example configures the enabling threshold and balancing threshold to 300 Kbps and 500 Kbps respectively for the same radios of AP devices in the AP group.

```
FS(config)# ap-group default
FS(config-group)# inter-radio-balance flow-balance same-band enable-load 3 threshold 5
```

The following example configures the enabling threshold and balancing threshold to 3 Mbps and 3 Mbps respectively for the same radios on all AP devices.

```
FS(config)# ap-config all
FS(config-ap)# inter-radio-balance flow-balance same-band enable-load 30 threshold 30
```

Related Commands

Command	Description

N/A	N/A

Platform Description

This command is supported only on ACs.

2.15 inter-radio-balance num-balance dual-band

Use this command to configure the enabling threshold and balancing threshold for STA balancing between the different radios (2.4G and 5.0G) of AP devices or AP groups. Use the **no** form of this command to restore the default settings.

inter-radio-balance num-balance dual-band enable-load *en-num* **threshold** *thrs-num*

no inter-radio-balance num-balance dual-band

Parameter Description

Parameter	Description
en-num	The enabling threshold value. Load balancing is enabled only when the number of STAs associated with the radio exceeds the threshold. The range is from 1 to 20.
thrs-num	The balancing threshold value. The STA will be disassociated with the radio when the STA number difference between the associated radio and lowest load radio. The range is from 1 to 20.

Defaults

By default, the enabling threshold is 8 and the balancing threshold is 8.

Command mode

AP /AP group configuration mode

Usage Guide

When the load balancing between radios is enabled, if the number of STAs associated with the radio exceeds the enabling threshold and the STA number difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the STAs will be balanced to radio of lower load. This configuration takes effect only when the radio of lowest load is on the different radio to be associated. The **inter-radio-balance num-balance same-band** takes effect If the two radios are on the same radio.

Configuration Examples

The following example configures the enabling threshold and balancing threshold to 10 and 10 respectively for the different radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# inter-radio-balance num-balance dual-band enable-load 10 threshold 10
```

The following example restores the default load balancing settings for different radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# no inter-radio-balance num-balance dual-band
```

The following example configures the enabling threshold and balancing threshold to 4 and 5 respectively for different radios of AP devices in the AP group.

```
FS(config)# ap-group default
FS(config-group)# inter-radio-balance num-balance dual-band enable-load 4 threshold 5
```

The following example configures the enabling threshold and balancing threshold to 5 and 5 respectively for different radios on all AP devices.

```
FS(config)# ap-config all
FS(config-ap)# inter-radio-balance num-balance dual-band enable-load 5 threshold 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.16 inter-radio-balance num-balance enable

Use this command to enable load balancing for the number of STAs between different radios (2.4G and 5.0G) on the AP device or AP group. Use the **no** form of this command to disable load balancing between radios on the AP device or AP group.

inter-radio-balance num-balance enable

no inter-radio-balance num-balance enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, load balancing between radios is disabled.

Command mode

AP /AP group configuration mode

Usage Guide

After load balancing between radios is enabled on an AP device, the AC device will make the STA number difference between radios on the AP device not exceed the threshold value.

Configuration Examples

The following example enables load balancing for the number of STAs between radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# inter-radio-balance num-balance enable
```

The following example disables load balancing for the number of STAs between radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# no inter-radio-balance num-balance enable
```

The following example enables load balancing for the number of STAs between radios on the AP devices in the default group.

```
FS(config)# ap-group default
FS(config-group)# inter-radio-balance num-balance enable
```

The following example enables load balancing for the number of STAs between radios on all AP devices.

```
FS(config)# ap-config all
FS(config-ap)# inter-radio-balance num-balance enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.17 inter-radio-balance num-balance same-band

Use this command to configure the enabling threshold and balancing threshold for STA balancing between the same radios (both 2.4G or 5.0G) of AP devices or AP groups. Use the **no** form of this command to restore the default settings.

inter-radio-balance num-balance same-band enable-load *en-num* **threshold** *thrs-num*

no inter-radio-balance num-balance same-band

Parameter Description

Parameter	Description
en-num	The enabling threshold value. Load balancing is enabled only when the number of STAs associated with the radio exceeds the threshold. The range is from 1 to 20.
thrs-num	The balancing threshold value. The STA will be disassociated with the radio when the STA number difference between the associated radio and lowest load radio. The range is from 1o to 20.

Defaults By default, the enabling threshold is 2 and the balancing threshold is 2.

Command mode AP /AP group configuration mode

Usage Guide When the load balancing between radios is enabled, if the number of STAs associated with the radio exceeds the enabling threshold and the STA number difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the STAs will be balanced to the radio of lower load. This configuration takes effect only when the radio of lowest load is on the different the radio to be associated. The **inter-radio-balance num-balance dual-band** takes effect If the two radios are on the different radio.

Configuration Examples

The following example configures the enabling threshold and balancing threshold to 3 and 3 respectively for the same radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# inter-radio-balance num-balance same-band enable-load 3 threshold 3
```

The following example restores the default load balancing settings for the same radios on AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# no inter-radio-balance num-balance same-band
```

The following example configures the enabling threshold and balancing threshold to 3 and 5 respectively for the same radios of AP devices in the AP group.

```
FS(config)# ap-group default
FS(config-group)# inter-radio-balance num-balance same-band enable-load 3 threshold 5
```

The following example configures the enabling threshold and balancing threshold to 5 and 5 respectively for the same radios on all AP devices.

```
FS(config)# ap-config all
FS(config-ap)# inter-radio-balance num-balance same-band enable-load 5 threshold 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.18 num-balance-group add

Use this command to add a specified AP to a specified load balancing group.

num-balance-group add *group-name ap-name*

Parameter Description

Parameter	Description
group-name	The name of the specified balancing group. Each number-based balancing group supports 10 APs at the most.
ap-name	The name of the AP to be added

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example adds ap1 to the balancing group test-group.

```
FS(config)# ac-controller
FS(config-ac)# num-balance-group add test-group ap1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.19 num-balance-group create

Use this command to create load balancing group based on number. Use the no form of this command to remove the configuration.

num-balance-group create *group-name*

no num-balance-group create *group-name*

Parameter Description

Parameter	Description
group-name	The name of the load balancing group, allows a maximum of 55 characters, blank space is not included. It supports 80 number-based balancing groups at most.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example creates a load balancing group named test-group.

```
FS(config)# ac-controller
FS(config-ac)# num-balance-group create test-group
```

The following example deletes a load balancing group named test-group.

```
FS(config)# ac-controller
FS(config-ac)# no num-balance-group create test-group
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.20 num-balance-group del

Use this command to delete a specified AP from a specified load balancing group.

num-balance-group del *group-name ap-name*

Parameter Description

Parameter	Description
group-name	The load balancing group for operation.
ap-name	The name of the AP to be deleted from the balancing group.

Defaults N/A

Command Mode The AC configuration mode

Usage Guide N/A

Configuration Examples

The following example deletes ap1 from the balancing group named test-group.

```
FS(config)# ac-controller
FS(config-ac)# num-balance-group del test-group ap1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.21 num-balance-group enable

Use this command to configure a threshold value for the number of STAs associated with AP devices to enable load balancing. Use the **no** form of this command to restore the default threshold value.

num-balance-group enable *group-name number*

no num-balance-group enable *group-name number*

Parameter Description

Parameter	Description
group-name	The load balancing group for operation.
ap-name	The enabling threshold value. The range is from 0 to 10. “0” indicates load balancing for the number of STAs is disabled.

Defaults The default enabling threshold is 3.

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example sets the enabling threshold for the number of STAs associated to 1.

```
FS(config)# ac-controller
FS(config-ac)# num-balance-group enable test-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.22 num-balance-group mode

Use this command to configure the mode of load balancing group. Use the **no** form of the command to restore the default setting.

num-balance-group mode *group-name* { **radio-mode** | **ap-mode** }

no num-balance-group mode *group-name*

Parameter Description

Parameter	Description
group-name	The name of the load balancing group for operation.
radio-mode	The radio-based mode of the load balancing group.
ap-mode	The AP-based mode of the load balancing group.

Defaults The default is AP-based mode.

Command Mode AC configuration mode.

Usage Guide N/A

Configuration Examples

The following example configures the radio-based mode for the balancing group named test-group

```
FS(config)# ac-controller
FS(config-ac)# num-balance-group mode test-group radio-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.23 num-balance-group num

Use this command to configure the load threshold of the load balancing group. Use the **no** form of this command to remove the configuration.

[no] flow-balance-group flow *group-name ap-name*

Parameter Description

Parameter	Description
group-name	The name of the load balancing group for the operation.
number	The threshold of balancing group. The range is from 0 to 20. 0 indicates this balancing group disables the flow-based load balancing function..

Defaults The default threshold is 3

Command Mode The AC configuration mode

Usage Guide N/A

Configuration The following example configures the threshold of the balancing group named test-group as 1.

Examples

```
FS(config)# ac-controller
FS(config-ac)# num-balance-group flow test-group 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.24 package

Use this command to create a terminal package and enter terminal package configuration mode. Use the **no** form of this command to restore the default setting.

package *pkg-name*

no package [*pkg-name*]

Parameter Description

Parameter	Description
pkg-name	Terminal package name. The name length range is from 1 to 32.

Defaults

No terminal packets are configured by default.

Command mode

Global configuration mode

Usage Guide

Up to 300 terminal packages can be configured on an AC. Only 50 terminal packages are allowed to be configured on a fat AP. The system will prompt an error message if the upper limit is exceeded.

Configuration Examples

The following example configures a terminal package named “Cart”1.

```
FS(config)#package Cart 1
FS(config-package)#
```

The following example configures the package named “Cart”1.

```
FS(config)# no package Cart 1
The operation will clear package(s) configuration, which may cause corresponding STAs offline. Continue? [no] y
FS(config)#
```

Related Commands

Command	Description
show package	Displays the terminal package configuration.

Platform Description

This command is supported only on ACs.

2.25 primary-sta

Use this command to configure a primary STA in a terminal package. Use the **no** form of this command to remove the configuration.

primary-sta *mac-address*

no primary-sta

Parameter

Parameter	Description

Description

mac-address	The MAC address of the primary STA, in the format of H.H.H.

Defaults N/A

Command mode Terminal package configuration mode

Usage Guide A terminal package can be configured up to one primary STA. Therefore the newly configured primary STA will cover the one which has been configured in a terminal packet.

Configuration Examples The following example configures a primary STA with MAC address of 00d0.f800.0001 for the terminal package "Cart 1".

```
FS(config)#package Cart 1
FS(config- package)#primary-sta 00d0.f800.0001
```

Related Commands

Command	Description
show package	Displays the terminal package configuration.

Platform Description This command is supported only on ACs .

2.26 secondary-sta

Use this command to configure secondary STAs in a terminal package. Use the **no** form of this command to remove the configuration**.**

secondary-sta *mac-address*

no secondary-sta [*mac-address*]

Parameter Description

Parameter	Description
mac-address	The MAC address of the secondary STA, in the format of H.H.H.

Defaults N/A

Command mode Terminal package configuration mode

Usage Guide Up to 100 secondary STAs can be configured in one terminal package. The system will prompt the error message in the following conditions if you use this command to configure the secondary STA:

The secondary STA configured has existed in the terminal package.

The number of STAs in a terminal package exceeds 100.

Configuration Examples The following example configures a secondary STA with MAC address of 00d0.f800.0002 for the package "Cart 1".

```
FS(config)#package Cart 1
FS(config- package)#secondary-sta 00d0.f800.0002
```

Related Commands

Command	Description
show package	Displays the terminal package configuration.

Platform Description This command is supported only on ACs.

2.27 show ac-config client

Use this command to display the information about all the STAs connected with the current AC.

show ac-config client [**by-ap-name** | **802.11a** | **802.11b** | **802.11n** | **802.11g** | **802.11ac |** **other**]

Parameter Description

Parameter	Description
by-ap-name	Indicates that the STAs are sorted by AP name.
802.11a	Displays information about users of 802.11a.
802.11b	Displays information about users of 802.11b.
802.11n	Displays information about users of 802.11n.
802.11g	Displays information about users of 802.11g.
802.11ac	Displays information about users of 802.11ac.
other	Displays information about unknown users.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the information about all the STAs connected with the current AC.

```
AC#show ac-config client
========= show sta status =========
AP      : ap name/radio id
Status: Speed/Power Save/Work Mode, E = enable power save, D = disable power save

Total Sta Num : 1
STA MAC          IP Address         AP                                          Wlan Vlan Status
Asso Auth Link Auth Up time
-------------- --------------- ---------------------------------------- ---- ---- ----------- --------- --------- -------------
78e4.00d3.1183 192.168.248.2      te/1                                        1       1       65.0M/D/bn
Open           Open             0:00:08:10
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.28 show ac-config client detail

Use this command to display the details of a specified wireless user.

show ac-config client detail *mac-addr*

Parameter Description

Parameter	Description
mac-addr	Indicates the MAC address of a wireless user.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the details of a specified wireless user.

```
AC#show ac-config client detail 0023.cdae.5260
Mac Address             :0023.cdae.5260
IP Address              :0.0.0.0
Wlan Id                  :123
Vlan Id                 :2
Roam State              :Local
Association ID          :0

Associated Ap Information:
AP Name                  :youzt
AP IP                   :10.1.1.2
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.29 show ap-config client-statistic

Use this command to display online/offline times and total roaming times in different. time.

show ap-config client-statistic

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the statistics about the specified wireless user.

```
AC# #show ac-config client statistic
========= show sta statistic =========
STA online    times in 5 second: 13
STA offline times in 5 second: 10
STA roaming times in 5 second: 2

STA online    times in 1 minute: 30
STA offline times in 1 minute: 25
STA roaming times in 1 minute: 10

STA online    times in 1 hour:      200
STA offline times in 1 hour:      300
STA roaming times in 1 hour:      100

Maxinum rate of STA-online in 1 hour: 20/s
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.30 show ac-config flow-balance summary

Use this command to display detailed configuration information of flow-based load balancing group.

show ap-config flow-balance summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays detailed configuration information of flow-based load balancing group.

```
FS(config)#show ac-config flow-balance summary
Group                  Threshold          AP NAME
--------------- -------------- --------------------------------------------------------------------------------
test-group1                 5*100kbps ap1, ap2, ap3
test-group2                 6*200kbps ap4, ap5, ap6
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.31 show ac-config num-balance summary

Use this command to display the detailed configuration information of the number-based load balancing group.

show ap-config num-balance summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the detailed configuration information of the number-based load balancing group.

```
FS(config)#show ac-config num-balance summary
Group                 Threshold AP NAME
---------------- --------- -------------------------
test-group1          1            ap1, ap2, ap3
test-group2          2            ap4, ap5, ap6
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.32 show assoc-control

Use this command to display the state of the association control.

show assoc-control

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the state of the association control.

```
FS# show assoc-control
Association control is enabled.
```

The following example displays the state of the association control.

```
FS# show assoc-control
Association control is disabled.
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.33 show control-zone

Use this command to display the association control-zone configuration.

show control-zone [**summary** | *czone-name*]

Parameter Description

Parameter	Description
summary	Displays summary information.
czone-name	The name of the association control-zone to be displayed. The name length range is from 1 to 64.

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

Use the **show control-zone summary** command to display the configured association control zone. Use the **show control-zone** or the **show control-zone czone-name** command to display not only the association control zone information but also the AP information in the control zone.

Configuration Examples

The following example displays all association control zones.

```
FS# show control-zone summary
control zone num :    4
Class 1 Grade 1
Class 2 Grade 1
Class 3 Grade 1
Class 1 Grade 2
```

The following example displays all association control zones.

```
FS# show control-zone summary
No control zone configuration.
```

The following example displays the detailed configuration information of all the association control zones.

```
FS# show control-zone
control zone num :    3
control-znoe               AP
-------------           ------------------------
Class 1 Grade 1                    AP1(1)-1    00d0.f800.889f
```

```
                              AP1(1)-2    00d0.f800.7869
Class 2 Grade 2                  AP2(2)-1    00d0.f800.889f
Class 3 Grade 3                  AP2(3)-1    offline
Class 3 Grade 2                  n/a
```

The following example displays the detailed configuration information of all association control zone.

```
FS# show control-zone
No control zone configuration.
```

The following example displays the detailed configuration information of the association control zone named "Class 1 Grade 1".

```
FS# show control-zone Class 1 Grade 1
control-zone            AP
-------------           ------------------------
Class 1 Grade 1                  AP1(1)-1    00d0.f800.889f
                              AP1(1)-2    00d0.f800.7869
Class 2 Grade 2                  AP2(2)-1    00d0.f800.889f
Class 3 Grade 3                  AP2(3)-1    offline
Class 3 Grade 2                  n/a
```

The following example displays the detailed configuration information of the association control zone named "Class 1 Grade 5".

```
FS# show control-zone Class 1 Grade 5
No such control zone configuration.
```

Related Commands

Command	**Description**
control-zone	Configures an association control zone and enter association control zone configuration mode.
ap	Configures AP information in the association control zone.

Platform Description This command is supported only on ACs.

2.34 show package

Use this command to display the terminal package configuration.

show package [*pkg-name*]

Parameter Description

Parameter	**Description**
pkg-name	The name of the terminal package to be displayed. The name length range is from 1 to 32.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration of all terminal packages.

```
FS# show package
```

```
total package num :    2
========= package_1 =========
primary STA :    none
secondary STA num :    0
========= package_2 =========
primary STA :    00d0.f809.0092
secondary STA num :    4
00d0.f809.0096
00d0.f809.0097
00d0.f809.0098
00d0.f809.0099
```

The following example displays the configuration of all terminal packages.

```
FS# show package
No package configuration
```

Related Commands

Command	Description
package	Enters terminal package configuration mode
primary-sta	Configures a primary STA.
secondary-sta	Configures a secondary STA.

Platform Description

This command is supported only on ACs.

2.35 show sta-blacklist

Use this command to display the STA blacklist.

show sta-blacklist

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the STA blacklist.

```
FS#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
```

Related Commands

Command	Description
N/A	N/A

Platform

This command is supported only on ACs.

Description

2.36 sta-balance num-limit enable

Use this command to enable the STA to terminate load balancing automatically after association failures. Use the **no** form of this command to restore the default setting.

sta-balance num-limit enable

no sta-balance num-limit enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command mode AC configuration mode

Usage Guide By default, the STA keeps attempting to associate e with the AP selected by load balancing. After the sta-balance function is enabled, the maximum number of its attempts is five times. If the association fails for five times, the STA will terminate load balancing next time.

Configuration Examples The following example enables the sta-balance function.

```
FS(config)# ac-controller
FS(config-ap)# sta-balance num-limit enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported only on ACs.

2.37 sta-blacklist

Use this command to enable the STA blacklist function, set aging time for the blacklisted STAs and identify the STA as the attack source. Use the **no** form of this command to restore the default setting.

sta-blacklist { **enable** | **lifetime** | **detect-time** | **fail-limit** } [*seconds* | *number*]

no sta-blacklist { **enable** | **lifetime** | **detect-time** | **fail-limit** } [*seconds* | *number*]

Parameter Description

Parameter	Description
enable	Enables the STA blacklist function.
lifetime	Sets aging time for the blacklisted STAs.
detect-time	Detection time. Once the STA fails to associate with the AP, it is identified as the attack source. If the STA association failure count reaches **fail-limit** within **detect-time**, the STA is added to the blacklist.
fail-limit	Limits the STA access failure count within **detec-time**.
seconds	In the unit of seconds. **lifetime**: in the range from 60 to 1200.

	detect-time: in the range from 5 to 60.
number	Sets the STA access failure count, in the range from 1 to 100.

Defaults

The STA blacklist function is disabled by default.

The default *lifetime* is 300 seconds.

The default *detect-time* is 60 seconds.

The default *number* is 5 seconds.

Command mode

AC configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the STA blacklist function.

```
FS(config)# ac-controller
FS(config-ac)# sta-blacklist enable
```

The following example disables the STA blacklist function.

```
FS(config)# ac-controller
FS(config-ac)# no sta-blacklist enable
```

The following example sets the blacklisted STA aging time to 60 seconds.

```
FS(config)# ac-controller
FS(config-ac)# sta-blacklist lifetime 60
```

The following example sets detect-time to 10 seconds.

```
FS(config)# ac-controller
FS(config-ac)# sta-blacklist detect-time 10
```

The following example limits association failure count.

```
FS(config)# ac-controller
FS(config-ac)# sta-blacklist fail-limit 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.38 sta-idle-timeout

Use this command to configure aging time for a wireless user in a specified AP or AP group. Use the **no** form of this command to restore the default setting.

sta-idle-timeout *timer-num*

no sta-idle-timeout

Parameter Description

Parameter	Description
timer-num	Indicates that you set the aging time, in the range from 60 to 86400 in the unit of seconds.

Defaults

The default is 300 seconds.

Command Mode

AP configuration mode/AP group configuration mode

Usage Guide

If no information is received from a wireless user within the setting time, the wireless user will be regarded to have left the WLAN, and will be deleted from the network by the system.

Configuration Examples

The following example enters the configuration mode of AP0001 to configure its client timeout timer to 600 seconds.

```
FS(config)# ap-config AP0001
FS(config-ap)# sta-idle-timeout 600
```

The following example enters the configuration mode of AP0001 to restore its client timeout timer to the default setting.

```
FS(config)# ap-config AP0001
FS (config-ap)# no sta-idle-timeout-timer
```

The following example enters the default AP group to configure its client timeout timer to 600 seconds.

```
FS(config)# ap-group default
FS (config-ap-group)# sta-idle-timeout 600
```

The following example enters the default AP group to restore its client timeout timer to the default setting.

```
FS(config)# ap-group default
FS(config-ap-group)# no sta-idle-timeout-timer
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.39 sta-limit

Use this command to configure the maximum number of wireless users that can be connected. In the AC configuration mode, this command can provide global configuration. In the AP group and AP configuration mode , this command can be used to configure the maximum number of wireless users that can be connected to a specified AP. In the WLAN configuration mode,this command can be used to configure the maximum number of wireless users that can be connected to a specified WLAN.Use the **no** form of this command to restore the default setting.

sta-limit *client-num*

no sta-limit *client-num*

Parameter Description

Parameter	Description
client-num	Indicates the maximum number of wireless users that can be connected. In the AC configuration mode: The value is equal to 32 multipled by the number of APs suppprted by the AC (depending on lincense limit) In the AP group configuration mode, the value is 512.

	In the AP configuration mode, for offline APs or ap-config all mode, the value is 512. For online APs, the value depends on the product model. In the WLAN configuration mode, the value is equal to 32 multipled by the number of APs suppprted by the AC (depending on lincense limit).

Defaults

In the AC configuration mode:

The default is equal to 32 multipled by the number of APs suppprted by the AC .

In theAP group configuration mode, the default is 32.

In the AP configuration modem, the default for the offline APs or ap-config all mode is 32 and the default for the online APs is determined by the AP model.

In the WLAN configuration mode, the default is no limit.

Command Mode

AC configuration mode

AP group configuration mode

AP configuration mode

WLAN configuration mode

Usage Guide

This command is used to configure how many clients the device can serve at most. This value should not exceed the maximum number supported by an AC or the maximum number limited by the license. The maximum number of wireless users that can be supported varies with AC products.

For the ap-config all, ap-group and off-line AP configuration, the range is from 1 to 512. If the value configured by the user exceed the STA number supported by an AP, it will automatically adjust the value to the maximum STA number supported by the AP when the AP is online.

For online APs, the maximum value is number of STAs supported by the AP.

Configuration Examples

The following example configures an AC to provide service for 2400 clients at most.

```
FS(config-ac)# sta-limit 2400
```

The following example configures all APs in the AP group (Default) to admit 20 wireless users at most.

```
FS(config)# ap-group default
FS(config-ap-group)# sta-limit 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.40 sta-limit per-ap

Use this command to configure the maximum number of STAs associated with each AP. Use the **no** form of this command to restore the default setting.

sta-limit per-ap *client-num*

no sta-limit per-ap

Parameter Description

Parameter	**Description**
client-num	Sets the maximum number of STAs associated with each AP in the range from 1 to 1536.

Defaults The default is no limit.

Command mode WLAN configuration mode

Usage Guide If the configured value exceeds the AP capacity, the AP capacity prevails.

Configuration Examples

The following example sets the maximum number of STAs associated with each AP in WLAN 1 to 10.

```
FS(config)# wlan-config 1
FS(config-wlan)# sta-limit per-ap 10
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

2.41 sta-limit radio

Use this command to configure the maximum number of wireless users that can be connected. In the AP group and AP configuration mode, you can specify the maximum number of wireless users connected on a specific radio of an AP. Use the **no** form of this command to restore the default setting.

sta-limit *client-num* **radio** *radio_id*

no sta-limit *client-num* **radio** *radio_id*

Parameter Description

Parameter	**Description**
client-num	Indicates the maximum number of wireless users that can be connected, in the range from 1 to 156 (or the maximum number of users supported by the AP).
radio-id	Indicates the radio identifier.

Defaults By default, there is no limit.

Command Mode AP configuration mode/ AP group configuration mode

Usage Guide

The limit number of user in this command has no dependence on that of the sta-limit command. In other words, the limit number of user in this command can be greater than that of the sta-limit command.

For the ap-config all, ap-group and off-line AP configuration, the range is from 1 to 156. If the value configured by the user exceed the STA number supported by an AP, it will automatically adjust the value to the maximum STA number supported by the AP when the AP is online.

For online APs, the maximum value is number of STAs supported by the AP.

Configuration Examples

The following example configures the maximum number of wireless users that can be added into radio 1 of an AP to 20.

```
FS(config)# ap-config ap1
FS(config-ap)# sta-limit 20 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

2.42 sta-logging rate-limit

Use this command to set the maximum number of syslogs printed per second, including STA online/offline information and STA change messages. Use the **no** form of this command to restore the default setting.

sta-logging rate-limit *limit-num*

no sta-logging rate-limit

Parameter Description

Parameter	Description
limit-num	Sets the maximum number of syslogs printed per second, in the range from 0 to 10000.

Defaults

The default is 5.

Command mode

AC configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the maximum number of syslogs printed per second to 100.

```
FS(config)# ac-controller
FS(config-ac)# sta-logging rate-limit 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported only on ACs.

3 WLAN CAPWAP Commands

3.1 ac-domain-name

Use this command to enable the AP to discover the AC domain name. Use the **no** form of this command to restore the default setting.

ac-domain-name *ac-domain-name*

no ac-domain-name

Parameter Description

Parameter	Description
ac-domain-name	Configures the AC domain name that the AP is to be discovered. The maximum length of the AC domain name is 64 characters, containing no spaces.

Defaults By default, the AC domain name is ac.FS.com.cn.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide AP is able to discover the AC through DNS. You can use this command to revise the AC domain name to be discovered by the AP, so as to allow the AP to discover different APs.

Configuration Examples

The following example enables the AP to discover the AC with the domain name as FS-ac.com.

```
FS(config)# ap-config AP001
FS(config-ap)# ac-domain-name FS-ac.com
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.2 acip ipv4

Use this command to configure the AP to join a specified AC. Use the **no** form of this command to remove the configuration.

acip ipv4 *ip-address* [*ip-address*]

no acip ipv4

Parameter Description

Parameter	Description
ip-address	Indicates the static IP address. Up to six static addresses can be configured.

Defaults N/A

Command Mode AP global configuration mode/AP configuration mode on the AC

Usage Guide

In general, the fit AP has no configuration. You can find AC through broadcast, multicast, DHCP and DNS or joining AC through the AC address configured by the static address. AP sends a discovery request packet to these IP addresses to detect whether AC is valid, and then add an AC.

⚠ If this command is configured for the fit AP and the AC connected with it, then the final configuration is the AC configuration.

Configuration Examples

The following example configures the static IP address list for the fit AP to join AC as 192.168.1.1 and 192.168.2.1.

```
FS(config)# acip ipv4 192.168.1.1 192.168.2.1
```

The following example configures the static IP address list for AP0001 to join AC as 192.168.1.1 and 192.168.2.1.

```
FS(config)# ap-config AP0001
FS(config-ap)# acip ipv4 192.168.1.1 192.168.2.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.3 active-bin-file

Use this command to activate an AP software version on an AC, and only the activated AP software version can be used to upgrade. Use the **no** form of this command to remove the configuration.

active-bin-file *filename* [**FSOS10**]

no active-bin-file *filename* [**FSOS10**]

Parameter Description

Parameter	Description
filename	Specifies software version name, including the suffix. This command can activate up to five software versions.
FSOS10	Activates the transition version between FSOS 10 to FSOS 11. The software only applies to the AP.

Defaults N/A

Command Mode AC configuration mode

Usage Guide

To configure an AC as the upgraded version of the specified AP product series, finish these three steps first: creating AP product series, configuring the software version corresponding to the specified AP, and activating the software version. Moreover, before the configuration, ensure this software version is available in the AC system files.

Configuration Examples

The following example activates an AP software version file ap.bin on the AC.

```
FS(config-ac)# active-bin-file ap.bin
FS(config-ac)#
```

The following example removes the activated AP software version file ap.bin from the AC.

```
FS(config-ac)# no active-bin-file ap.bin
```

Related Commands

Command	Description
ap-serial	Creates an AP product series name and specify which hardware version AP product models belong to this series.
ap-image	Upgrades a specified AP software version with a specified activated file.

Platform Description N/A

3.4 ap-image

Use this command to configure AC upgrade to use a specified file to upgrade a specified series of APs. This command applies to all APs connected to the current AC. Use the **no** form of this command to remove the configuration.

ap-image { **auto-upgrade** | *filename serial-name* }

no ap-image { **auto-upgrade** | *filename serial-name* }

Parameter Description

Parameter	Description
auto-upgrade	Automatically matches the proper AP for upgrade.
filename	Indicates a software version name, including the suffix.
serial-name	Indicates the AP model series to be upgraded.

Defaults N/A

Command Mode AC configuration mode

Usage Guide

This command is intended to use a specified file to upgrade a specified series of APs. This command applies to all APs connected to the current AC. To configure an AC as the upgraded version of the specified AP product series, finish these three steps first: creating AP product series, configuring the software version corresponding to the specified AP, and activating the software version. Moreover, before configuration, ensure this software version exists in the AC system files.

Configuration Examples

The following exmaple configures the product series name as **test-serial**, and upgrades it with the **ap.bin** file.

```
FS(config-ac)# ap-serial test-serial AP210-E, AP210, AP220-E, AP220 hw-ver 1.0
FS(config-ac)#
FS(config-ac)# ap-image ap.bin test-serial
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.5 ap-image

Use this command to upgrade a specified AP with a specified file. This command does not support the ap-config all mode. Use the **no** form of this command to remove the settings.

ap-image *filename*

no ap-image

Parameter Description

Parameter	Description
filename	Specifies an AP software version filename for upgrade, including the suffix.

Defaults

N/A

Command Mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following exmaple upgrades AP0001 with the file **ap.bin**.

```
FS(config-ac)# ap-serial test-serial 1.0 AP220-E hw-ver 1.0
FS(config-ac)# active-bin-file ap.bin
FS(config-ac)# exit
FS(config)# ap-config AP0001
FS(config-ap)# ap-image ap.bin
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.6 apip ipv4

Use this command to configure a static IP address for a specified AP. Use the **no** form of the command to remove the configuration.

apip ipv4 *ip-address network-mask gateway*

no apip ipv4

Parameter Description

Parameter	Description
ip-address	The static IP address.
network-mask	The subnet mask.
gateway	The gateway address.

Defaults N/A

Command Mode AP global configuration mode

Usage Guide

In general, the fit AP has no configuration. Its IP address and gateway can be dynamically obtained by DHCP. When the CAPWAP tunnel between AP and AC is established, AC delivers the static IP address for AP, so that the address of AP maintains unchanged after AP is rebooted. In special application scenario, you can configure this command in AP global configuration mode to manually set the static IP address for the fit AP.

⚠ 1. With the AP address configured as static, the DHCP is disabled, and the AC address cannot be obtained through the OPTION of DHCP. Therefore, after this command is configured, you need to configure the AC address using the command “acip” on the AP so that the AP can find and join the AC when the AP and the AC are not in the same subnet.

2. The configuration of this command will be automatically saved after the AP configuration. No command of saving is required to be executed.

3. This command serves the same purpose as the command “ip address” on the AC in the AP configuration mode. However, when the AP joins the AC, if the command “ip address” exists in the AP configuration mode of the AC and conflicts with the command “apip”, the static address of the AP will be updated and the CAPWAP tunnel will be re-created.

Configuration Examples

The following example configures the static IP address of the fit AP as 192.168.1.2, the subnet mask as 255.255.255.0, and the gateway as 192.168.1.1..

```
FS(config)# apip ipv4 192.168.1.2 255.255.255.0 192.168.1.1
```

Related

Command	Description

Commands

acip	Specifies the AC address to be connected with by an AP.
ip address	Configures the static address of the AP.

Platform Description

N/A

3.7 apip pppoe

Use this command to enable the AP to obtain the address through PPPoE. Use the **no** form of this command to restore the default setting.

apip pppoe

no apip pppoe

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

AP global configuration mode

Usage Guide

After configuring this command, you should perform PPPoE and configure the default route to point to the dialer interface to enable communication between the AP and the AC.

⚠ CAPWAP can select only dialer 1 as the source port. Therefore, PPPoE dial requires dialer 1.

Configuration Examples

The following example enables the fit AP to obtain the address through PPPoE.

```
FS(config)# apip pppoe
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.8 ap-serial

Use this command to configure an AP series on an AC. Only when the AP hardware version and product model are configured to a series can its software version be upgraded through the AC. Use the **no** form of this command to remove the configuration.

ap-serial *serial-name hardware-version ap-pid1, ap-pid2, ..., ap-pidn* [**hw-ver** *hardware-version*]

no ap-serial *serial-name*

Parameter Description

Parameter	Description
serial-name	Indicates an AP series name to be created. The maximum character configuration number is 64, blank space is not included. The maximum number of the AP series that can be supported at the same time: WS5708 series: 16, WS5302 series:8
ap-pid1 ap-pid2 ... ap-pidn	Product models
hardware-version	Indicates the AP hardware version, the maximum configuration character is 64, blank space is not included. The hardware version name is a decimal, the mark is 'x' or 'X" which can be used to configure the following character.

Defaults

N/A

Command Mode

AC configuration mode

Usage Guide

To configure an AC as the upgraded version of the specified AP product series, finish these three steps first: creating AP product series, configuring the software version corresponding to the specified AP, and activating the software version. Moreover, before configuration, ensure this software version exists in the AC system files.

Configuration Examples

The following example creates an AP series named **test-serial** of which the designate AP hardware version is 1.0 on an AC, including these AP models: AP220-SE AP220-SH, AP220-E.

```
FS(config-ac)# ap-serial test-serial 1.0 AP220-SE AP220-SH, AP220-E hw-ver 1.0
FS(config-ac)# active-bin-file ap.bin
FS(config-ac)# ap-image test-serial ap.bin
```

The following exmaple removes the configuration from the AC to make the APs in the product series named **test-serial** no longer use the **ap.bin** file for upgrade.

```
FS(config-ac)# no ap-image test-serial ap.bin
```

Related Commands

Command	Description
active-bin-file	Activates an AP software version file to upgrade an AP software version.

Platform Description

N/A

3.9 ap-subif

Use this command to enable the AP to create the sub interface of the WAN port. Use the **no** form of this command to remove the configuration.

ap-subif enable

no ap-subif enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode AP configuration mode

Usage Guide If the AP obtains its address through PPPoE, the sub interface of the WAN port is removed automatically. This command cannot enable the AP to create the sub interface of the WAN port in PPPoE mode.

Configuration Examples The following example enables AP1 to remove the sub interface from the WAN port.

```
FS(config)# ap-config AP1
FS(config-ap)# no ap-subif enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.10 ap-vlan

Use this command to set the Native VLAN for the AP. Use the **no** form of this command to restore the default setting.

ap-vlan *vlan-id*

no ap-vlan

Parameter Description

Parameter	Description
vlan-id	Specifies the VLAN on the wired network port, in the range from 1 to 4094.

Defaults The default is 1.

Command Mode AP configuration mode

Usage Guide The AP untags the frame of the Native VLAN before forwarding it. In local forwarding mode, if the user VLAN is the same as the Native VLAN, the frame is forwarded untagged and the access switch determines the VLAN where the user resides.

⚠ This command forces the online AP to go offline and enables reconnection.

⚠ In WDS deployment, when ROOT-BRIDGE and NONROOT-BRIDGE devices are configured with local forwarding, they should reside in the same AP-VLAN. Otherwise, the NONROOT-BRIDGE device cannot share the address pool with the ROOT-BRIDGE device; packet forwarding on the NONROOT-BRIDGE device may even be affected.

⚠ This command is configured only when the STA of a WLAN wants to access the VLAN where the switch resides while another WLAN requires that its STA resides in VLAN 1, which is not the Native VLAN.

⚠ If the static DHCP address pool is configured, and BVI 1 port number is used as client ID, this configuration will bring changes to the BVI port. In this case, the DHCP server configuration should be modified. Otherwise, the address cannot be obtained.

⚠ When the AP obtains the address through PPPoE and CAPWAP selects dialer 1 as the source port, the STA traffic is forwarded untagged even if this command is configured.

Configuration Examples

The following example sets the Native VLAN for AP 1 to 20.

```
FS(config)# ap-config AP1
FS(config-ap)# ap-vlan 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.11 ap-upgrade bandwidth

Use this command to configure the upgrade bandwidth for AP devices. Use the **no** form of this command to restore the default setting.

ap-upgrade band-width *num*

no ap-upgrade band-width

Parameter Description

Parameter	Description
num	Bandwidth for AP upgrade, namely, the push rate for the AP upgrade file. The range is from 1 to 1,024. The unit is 1 KB. The default value is 0.

Defaults

Upgrade bandwidth is not limited by default.

Command Mode

AP configuration mode

Usage Guide

During upgrading AP devices, the AC device occupies more transmission bandwidth to reduce upgrade time. However, in some small networks, the bandwidth for wired services should be guaranteed during AP upgrade to avoid impacting wired services. You can configure the upgrade bandwidth for AP devices to control the percentage of upgrade bandwidth.

The bandwidth limit configured

1. This command configuration controls the bandwidth for centralized upgrade of AP devices from the AC device, the distributed upgrade of AP devices is not impacted. As distributed upgrade data source is from central upgrade, the distributed upgrade is indirectly influenced.
2. The bandwidth unit is 1KB. For example, the minimum link bandwidth between AC and AP devices is 1 Mbps, the bandwidth value is 128.

Configuration Examples

The following example sets the upgrade bandwidth for an AP device to 1 Mbps.

```
FS(config-ac)# ap-upgrade band-width 128
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description

N/A

3.12 ap-upgrade group

Use this command to add an AP device to the upgrade group. Use the **no** form of this command to remove the AP device from the upgrade group.

ap-upgrade group *group-name*

no ap-upgrade group

Parameter Description

Parameter	**Description**
group-name	Upgrade group name.

Defaults

N/A

Command Mode

AP configuration mode

Usage Guide

The following configuration restrictions are applied on the AP devices which are added to a upgrade group:

1. The AP devices in the same group need to be configured with the **ap-grade band-width** command, so that the upgrade bandwidth of the AP devices is identical.
2. The **capwap upgrade group** command should be configured before this command.

Configuration

The following example adds an AP device to the upgrade group UPGRADE-GROUP1.

Examples

```
FS(config-ac)# ap-upgrade group UPGRADE-GROUP1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A.

3.13 capwap ctrl-ip

Use this command to set the IPv4 address for the CAPWAP tunnel between the AC and the AP. Use the **no** form of this command to restore the default setting.

capwap ctrl-ip *ip-address*

no capwap ctrl-ip

Parameter Description

Parameter	Description
ip-address	Specifies the IP address for the CAPWAP tunnel between the AC and the AP. It should be an interface IP address of the AC.

Defaults

Command Mode

AC configuration mode

Usage Guide

The AC generally uses a Loopback address to create the CAPWAP tunnel. This command enables the AC to create the CAPWAP tunnel with interface addresses in other three layers.

⚠ This command may force the AP offline.

⚠ Configuring an IP address not existing on the AC causes failure to create the CAPWAP tunnel.

⚠ If the gateway of the AP is not on the AC, the AP address pool option should be set to the IP address in this command (if it is configured).

⚠ In the AC hot backup environment, if this command is used to set the CAPWAP tunnel address, use the **peer-ip A.B.C.D** command to set the same IP address on the peer-to-peer backup AC.,

Configuration Examples

The following example sets the IP address for the CAPWAP tunnel between the AC and the AP to 10.0.0.1..

```
FS(config-ac)# capwap ctrl-ip 10.0.0.1
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

3.14 capwap dtls enable

Use this command to enable DTLS encryption for the CAPWAP tunnel. Use the **no** form of this command to disable this function.

capwap dtls enable

no capwap dtls enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command Mode AC configuration mode

Usage Guide This function is enabled by default to ensure security of communication between the AC and the AP. This function is disabled in some cases, for example, for test purpose.

Configuration Examples The following example enables DTLS encryption for the CAPWAP tunnel.

```
FS(config)# ac-controller
FS(config-ac)# capwap dtls enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.15 capwap fragment enable

Use this command to enable CAPWAP fragmentation. Use the **no** form of this command to restore the default setting.

capwap fragment enable

no capwap fragment enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

AP configuration mode/AP group configuration mode

Usage Guide

After the packets are encapsulated through the CAPWAP tunnel, its length may exceed IP MTU, causing IP fragmentation. If IP MTUs of multiple nodes on a link are inconsistent, the packet may go through fragmentation and defragmentation for many times, affecting packet forwarding. This command is used to enable CAPWAP fragmentation, that is, the packet is fragmented during CAPWAP encapsulation. The length of fragmented packets can be set to the minimum MTU using the **capwap mtu** command to avoid another IP fragmentation.

Configuration Examples

The following example enables CAPWAP fragmentation on AP1.

```
FS(config)# ap-config AP1
FS(config-ap)# capwap fragment enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.16 capwap max-concurrent

Use this command to set the maximum number of concurrent online APs. Use the **no** form of this command to restore the default setting.

capwap max-concurrent *num*

no capwap max-concurrent

Parameter Description

Parameter	Description
num	The maximum number of concurrent online APs, in the range from 1 to 200.

Defaults

The default is 50.

Command Mode

AC configuration mode

Usage Guide

If too many APs go online concurrently, AC CPU may increase even to 100%. This will cause the tunnel disconnection. Therefore, it is necessary to limit the number of concurrent online APs.

⚠ If you set a small value, the total online time of all APs associated to the AC will be long.

Configuration Examples

The following example sets the maximum number of concurrent online APs to 100.

```
FS(config-ac)#capwap max-concurrent 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.17 capwap max-retransmit

Use this command to set the maximum count of CAPWAP packet retransmission. Use the **no** form of this command to restore the default setting.

capwap max-retransmit *num*

no capwap max-retransmit

Parameter Description

Parameter	Description
num	Sets the maximum count of CAPWAP packet retransmission, in the range from 3 to 60.

Defaults

The default is 5.

Command Mode

AP configuration mode/AP group configuration mode

Usage Guide

If the CAPWAP request packet is not responded, the packet is retransmitted, The retransmission interval increases by the initial retransmission interval (the smaller value between three seconds and half echo-interval) and the maximum retransmission interval should be no greater than the smaller value between half echo-interval and 60 seconds. If the device does not receive the response packet within the maximum count, the tunnel is considered disconnected. This command is only effective when the tunnel is in the Run state.

Configuration Examples

The following example sets the maximum retransmission count to 20.

```
FS(config)# ap-config AP1
FS(config-ap)#capwap max-retransmit 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.18 capwap upgrade group

Use this command to configure an AP upgrade group. Use the **no** form of this command to remove an AP upgrade group.

capwap upgrade group *group-name* [**max-concurrent** *num*]

no capwap upgrade group [*group-name* **max-concurrent**]

Parameter Description

Parameter	Description
num	The number of AP devices which can be upgraded concurrently in centralized mode. The range is from 1 to 200. The default is 5.
group-name	Upgrade group name

Defaults

Command Mode AC configuration mode

Usage Guide The AP number should be equal to the available bandwidth divided by max bandwidth of each AP.

Configuration Examples The following example creates an AP upgrade group Upgrade-Group1 and sets the concurrent number to 10.

```
FS(config-ac)# capwap upgrade group Upgrade-Group1 max-current 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.19 capwap mtu

Use this command to set the Path MTU (PMTU) for the CAPWAP tunnel. Use the **no** form of this command to restore the default setting.

capwap mtu *num*

no capwap mtu

Parameter Description

Parameter	Description
num	Sets the PMTU for the CAPWAP tunnel, in the range from 68 to 1500 in the unit of bytes.

Defaults The default is 1500.

Command Mode

AP configuration mode/AP group configuration mode

Usage Guide

If the CAPWAP-encapsulated packet is longer than the PMTU, the packet is fragmented. Set the PMTU equal to the maximum IP MTU so as to avoid IP fragmentation and defragmentation.

⚠ A small PMTU will produce a large quantity of packet fragments, affecting packet forwarding or even leading to transmission failure. It is recommended to set a reasonable PMTU.

Configuration Examples

The following example sets the PMTU for the CAPWAP tunnel to 1200 bytes.

```
FS(config)# ap-config AP1
FS(config-ap)# capwap mtu 1200
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A.

3.20 capwap upgrade max-concurrent

Use this command to set the maximum number of concurrently upgrading APs. Use the **no** form of this command to restore the default setting.

capwap upgrade max-concurrent *num*

no capwap upgrade max-concurrent

Parameter Description

Parameter	Description
num	The maximum number of concurrently upgrading APs, in the range from 1 to 200.

Defaults

The default is 15.

Command Mode

AC configuration mode

Usage Guide

If too many APs upgrade concurrently, AC CPU may increase even to 100%. This will cause tunnel disconnection. Therefore, it is necessary to limit the number of concurrently upgrading APs.

Configuration Examples

The following example sets the maximum number of concurrently upgrading APs to 10.

```
FS(config-ac)#capwap upgrade max-concurrent 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.21 echo-interval

Use this command to configure the keep-alive interval for CAPWAP. Use the **no** form of this command to restore the default setting.

echo-interval *seconds*

no echo-interval

Parameter Description

Parameter	Description
seconds	This parameter indicates the keep-alive interval for CAPWAP, in the range from 5 to 255 in the unit of seconds.

Defaults The default is 30 seconds.

Command Mode AP configuration mode or AP group configuration mode

Usage Guide

In the fit AP network frame, AC and AP are connected through the CAPWAP tunnel. Echo Request and Echo Response are used to keep the validity of the link. In the case of no other request packets, AP sends the Echo Request packet to keep alive every echo interval. If AP does not receive a response, the packet will be retransmitted at the multiple original retransmission interval (3 seconds or half the echo interval, taking the smaller value) and the longest retransmission interval cannot exceed half the echo interval or 60 seconds (taking the smaller value). It is considered that the tunnel is interrupted if the AP does not receive the response packet within the maximum retransmit times, which means the failure time of keep alive of the tunnel is the keep-alive time plus retransmission intervals. This command only takes effect in the Run status of the tunnel. By default, the echo-interval is 30 seconds, the maximum retransmit times are 5. Namely, the AP device sends a request and does not receive a response after 0 second, the request packet will be retransmitted at the interval of 3 seconds, 6 seconds, 12 seconds, 15 seconds and 15 seconds.

⚠ In the deployment of wireless networks, you can adjust the echo interval based on network size to plan the convergence capability of the network. During the adjustment, make sure that you know the network size and the network does require the convergence capability to prevent impacts on the network environment due to too low value in the wireless network deployed by massive APs.

Configuration Examples

The following exmaple configures a 10-second echo interval for AP0001.

```
FS(config)# ap-config AP0001
FS(config-ap)# echo-interval 10
```

The following example configures a 10-second echo interval for all APs.

```
FS(config)# ap-config all
FS(config-ap)# echo-interval 10
```

The following example configures a 10-second echo interval for all APs in the default AP group.

```
FS(config)# ap-group default
FS(config-ap-group)# echo-interval 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.22 exec-cmd

Use this command to configure an AP to execute a command. Use the no form of this command to remove the setting.

exec-cmd mode *exec-mode* **cmd once**

no exec-cmd mode *exec-mode* **cmd** *exec-cmd*

Use this command to configure all APs in an AP group to execute a command.

no exec-cmd mode *exec-mode* **cmd** *exec-cmd*

Parameter Description

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	Indicates that the command is executed only once and is not saved.

Defaults

N/A

Command Mode

Single AP configuration mode/All APs configuration mode/AP group 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. If **ap-config all** and **ap-config** are configured simultaneously, for online APs, the later configuration will take effect; for offline APs, **ap-config** has a higher priority than **ap-config all**.

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.

Configuration Examples

The following example disables Eweb for an AP.

```
FS(config)#ap-config AP1
FS(config-ap)# exec-cmd mode configure cmd "no enable service web-server all"
```

The following example enables Eweb for an AP,

```
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"
```

The following example configures Bluetooth iBeacon for all APs in the AP group.

```
FS(config)#ap-group default
FS(config-group)#exec-cmd ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff
```

The following example disables Eweb for all APs in the AP group.

```
FS(config-group)#exec-cmd exec-cmd mode configure cmd "no enable service web-server all"
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.23 ip address

Use this command to configure the static IP address of a specified AP. Use the **no** form of this command to restore the default setting.

ip address *ip-address network-mask gateway*

no ip address

Parameter Description

Parameter	Description
ip-address	Interface address of the AP.
network-mask	Address mask of the AP.
gateway	Gateway of the AP.

Defaults

N/A

Command Mode

AP configuration mode

Usage Guide

The AP can obtain its IP address through static configuration or DHCP. If the AP has not a static IP address, it will obtain an address dynamically by DHCP and join the AC. In this case, you can use this command to configure the static address of the AP so that the address keeps unchanged after the AP restarts.

⚠ 1. With the AP address configured as static, the DHCP is disabled, and the AC address cannot be obtained through the OPTION of DHCP. Therefore, before this command is configured, you need to configure the address of the AC connected by using the command "acip" in AP configuration mode so that the AP can find and join the AC when the AP and the AC are not in the same subnet.

2. If the current address of the AP is not the same as the one specified through this command, the static address will be updated and the CAPWAP tunnel will be re-created.

Configuration Examples

The following example configures the address of AP0001 as 1.1.1.1, its mask as 255.255.255.0, and its next hop as 1.1.1.2.

```
FS(config)# ap-config AP0001
FS(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2
```

Related Commands

Command	Description
apip	Configures the static address of an AP on the AP.
acip	Specifies the AC address to be connected with by an AP.

Platform Description

N/A

3.24 link-latency

Use this command to check the link status between an AC and the APs in a specified AP group. Use the **no** form of this command to remove the configuration.

[**no**] **link-latency**

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

AP configuration mode/AP group configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables inspection of the link status between specified AP-0001 and an AC, and check information about the corresponding link status.

```
FS(config)#ap-config AP-0001
FS(config-ap)#link-latency
```

The following example enables inspection of the link status between an AC and the APs in the **default** AP group, and check the link status information about the specified AP-0001.

```
FS(config)# ap-group default
FS(config-ap-group)# link-latency
```

Related Commands

Command	Description
show ap-config link-latency	Checks link status between AC and AP.

Platform Description

N/A

3.25 location

Use this command to configure information about AC and AP location. Use the **no** form of this command to restore the default setting.

location *location-string*

no location

Parameter Description

Parameter	Description
location-string	Indicates AC location information, which can consist of up to 255 characters without any space.

Defaults

By default, the AC location information is FS_COM, the AP location information is null.

Command Mode

AC configuration mode/AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the location of a specific AC to the second floor of the computer department building (computer-layer2).

```
FS(config-ac)# location computer-layer2
```

The following example configures AP0001 location information to AP-company.

```
FS(config)# ap-config AP0001
FS(config-ap)# location AP-company
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.26 set version

Use this command to set the version number.

set-version *string*

Parameter Description

Parameter	Description
string	Sets the version number.

Defaults N/A

Command Mode AC configuration mode

Usage Guide This command is used to set the version number and push version number to APs.

Configuration Examples The following example sets the version number to FSOS 10.4(2B17)-SP2.

```
FS(config)# ac-controller
FS(config-ac)# set-version FSOS 10.4(2B17)-SP2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.27 show ac-config active-file

Use this command to display a list of activated files on the current AC. The **Used** field indicates how many APs are using this file, and the **Ready** field indicates whether this file has been activated completely.

show ac-config active-file

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays a list of activated files on the current AC.

```
FS#show ac-config active-file
Cnt    File Name                        Image Id           Software number        Type
Used Cnt    DL Cnt Ready
```

```
------ ---------------------------------- -------------------- -------------------- ---------- ---------- ---------- --------
1          ap220ev1.1-mid(6-3).bin                     FSOS 10.X-UPG              NA                            FSOS10
0              0                  Init
2         ap220.bin                                    1.0.0.017ed304            M09092708272014          main
0              0                  Init
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.28 show ac-config serial-product

Use this command to display the correspondence association between the AP product series and product models configured of the AC, and display which files should be used to upgrade the corresponding product series.

show ac-config serial-product

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the AP product series and product models configured for the current AC.

```
FS#show ac-config serial-product


Cnt       Serial Name         Hardware Version File Name        AP Product ID

------ --------------- ---------------- ------------ ---------------

1          ap-ser1.x            1.x                        ap220-1.bin    AP220-E

                                                                             AP220-SE

                                                                             AP220-SH

                                                                             AP620-H
```

```
                                                      AP220-E(M)

2       ap-ser2.x       2.x             ap220.bin   AP220-E

                                                      AP220-SH

                                                      AP220-E(M)
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.29 show ac-config upgrade-group

Use this command to display the upgrade groups and AP devices on the AC device.

show ac-config upgrade-group [*group-name*]

Parameter Description

Parameter	Description
group-name	AP upgrade group name.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays AP upgrade groups.

```
FS#show ac-config upgrade-group
Cnt    Group-Name                      Max-Concurrent    Token cnt    Upgrading cnt
------ --------------------------------- ------------ ----------- ------------
1      UPGRADE-GROUP1                       10               2            1
```

The following example displays the AP devices in the upgrade group.

```
FS#show ac-config upgrade-group UPGRADE-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
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

3.30 show ap-config board-data

Use this command to display the board data information of an AP.

show ap-config board-data *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the board data information of an AP.

```
ac#show ap-config board-data wlan-ap-0001
Ap(wlan-ap-0001)'s board data:
wtp model num              :
    wtp serial num          :1234567890123
    board id                  :AP220E
    board reversion         :AP2
    base address           :0011.2233.4455
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.31 show ap-config inventory

Use this command to display the manufacturer information about an AP.

show ap-config inventory *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the manufacturer information of an AP.

```
ac#show ap-config inventory wlan-ap-0001
AP Name: wlan-ap-0001
Location:
Product Id: AP220E
Vendor Id: 31762
SN: 1531991320
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.32 show ap-config link-latency

Use this command to check the link status between AC and AP.

show ap-config link-latency {all | single *ap-name*}

Parameter Description

Parameter	Description
all	Indicates that you check the link status information of all APs associated with the AC.
single *ap-name*	Indicates that you check the link status information of a single AP.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the link status information of the specified AP-0001.

```
FS(config)#show ap-config link-latency single AP-0001
```

```
AP Name     Status          Current       Maximum      Minimum
--------- ----------- ---------- --------- ---------
AP-0001     Enabled         4            ms 22         ms 2           ms
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.33 show ap-config reboot

Use this command to display the reboot information about an AP.

show ap-config reboot *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the reboot information of an AP.

```
ac#show ap-config reboot wlan-ap-0001
Ap(wlan-ap-0001)'s reboot statistic:
Reboot Cnt                   :0
AC Init Cnt                :0
Link Fail Cnt            :0
SW Fail Cnt                 :0
HW Fail Cnt                  :0
Other Fail Cnt           :0
Unknow Fail Cnt         :0
Last Fail Type           :0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.34 show ap-config static-ip

Use this command to display static address information on the AP.

show ap-config static-ip { **all** | **single** *ap-name* }

Parameter Description

Parameter	Description
all	Displays all APs.
single	Displays one single AP.
ap-name	The AP name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays static address information, including the AP name. IP address, network mask and gateway.

```
FS#show ap-config static-ip single 0034.5612.78a0
AP Name          Static IP      Net Mask                    Getway
----------------------------------------------------------------- ---------------
0034.5612.78a0                  Enabled 22.22.22.22    255.255.255.0     22.22.22.53
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.35 show ap-config summary location

Use this command to display location information on all APs.

show ap-config summary location

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays location information on all APs, including the AP name, MAC address, location, and status (online/offline).

```
FS#show ap-config summary location
AP Name                                    IP Address        Mac Address       Location
State
--------------------------------------- --------------- -------------- ---------------------------------------- -----
ap220                                      172.18.100.4      1414.4b13.9ff3    Bangongshi_4#
Run
ap3                                        172.18.100.16     001a.a94e.d40d    building 20#3F
Run
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.36 show ap-config updating-list

Use this command to display upgrade information on the AP.

show ap-config updating-list

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays upgrade information on the AP.

```
FS#show ap-config updating-list
AP NAME                              AP PID              File Tx   Time        AP Reset Ready
-------------------------- --------------- -------- -------- ---------------
AP220-I                           AP220-I              100        00:00:45    Y
```

```
00d0.1414.3f67          AP220-E          98          00:00:48    N
```

Field	Description
AP NAME	AP name.
AP PID	AP ID.
File Tx	File transfer process.
Time	Upgrade duration.
AP Reset Ready	Resets after upgrade is complete.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.37 show ap-config wtp-descriptor

Use this command to display the status description of an AP.

show ap-config wtp-descriptor *ap-name*

Parameter Description

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the status description of an AP.

```
ac#show ap-config wtp-descriptor wlan-ap-0001
Ap(wlan-ap-0001)'s wtp descriptor:
max radio              :2
radio in used          :2

encrypt num            :2
Cnt    WBID      Encry Cap
1      0x1       0xc

sub descriptor num    :3
Cnt    vonder id version type     version len       version
1      0x7c12      BOOT Ver          28                    MainVer10.SubVer4.SvnVer3634
```

```
2      0x7c12      ACT SW Ver        30                    FSOS 10.4 (1t7)(1T7), Release(73413)
3      0x7c12      HW Ver             3                     1.0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.38 show ap-config wtp-info

Use this command to display the AP device status.

show ap-config wtp-info *ap-name*

Parameter Description

Parameter	Description
ap-name	AP device name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the AP device status.

```
FS#show ap-config wtp-info ap220e
Ap(ap220e)'s status:
AC IP(status):          :101.101.101.101
AP IP(status):          :10.10.10.8 255.255.255.0 10.10.10.2
AP IPV6(status):        :::/0 ::
AP IPV4 ENABLE:           :enable
Location Data:            :
Session ID:               :88320000,111163fb,5c3b3cb3,2cac585a
mac type                     :full support
WTP Name:                     :ap220e
AP Domain Name:          :ac.FS.com.cn
wired vlan                  :0 port id 1
wired vlan                  :0 port id 2
wired vlan                  :0 port id 3
wired vlan                  :0 port id 4
Cw_interface_name      :BVI 1
Cw_wan_interface_ifx::1
Cw_wan_interface_ifx::0
```

```
Upgrading State          :Init
AP Image file            :NA
Real version             :1.0.0.641d31e6
Custom version           :AP_FSOS 11.1(2)B1
Upgrade version          :NA
Upgrade from AP          :FALSE
Upgrade for other AP:FALSE
Upgrade from AC          :FALSE
Wait for upgrade         :FALSE
Support distr-upg        :TRUE
Upgrade-banfwidth        :128
Upgrade group            :Upgrade-group1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.39 show capwap detail

Use this command to display details about the CAPWAP tunnel.

show capwap [*index* | [*ip-address* [*port*]]] **detail**

Parameter Description

Parameter	Description
index	Tunnel index.
ip-address	Tunnel IP address.
port	Tunnel port number.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays details about the CAPWAP tunnel whose address is 1.1.1.1.

```
FS#show capwap 1.1.1.1 detail
CAPWAP process “capwap 1” with state Run
  Process uptime is 3 days 0 hour 41 minutes
  Echo interval is 30 secs, Dead interval is 81 secs
```

```
Current timers echo-interval
Peer address is 172.18.59.5
Peer control port is 10000, data port is 10001
My address is 55.55.55.60
The MAC of AP is 001a.a94e.d773
The Session ID of AP is 001a.a94e.d773.53e1.0801.53e1.0801.53e1
The Path MTU is 1500
Recent recieved request's sequence number 39
Recent recieved response's sequence number 11
Recent send request's sequence number 11
Retransmit Count 0, Discovery Count 0, Failed DTLS Session Count 0
Sending queue length 0, Receive queue length 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.40 show capwap state

Use this command to display the CAPWAP tunnel state.

show capwap state

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the CAPWAP tunnel state.

```
FS#show capwap state
CAPWAP tunnel state, 3 peers, 2 is run:
Index   Peer IP                 Peer Port   State          Mac Address
1       192.168.0.1             10000       Run            001a.a900.0001
2       192.168.0.2             10000       Run            001a.a900.0002
```

```
3          192.168.0.3                    10000          DTLS Teardown       001a.a900.0003
```

Field	Description
Index	Tunnel index.
Peer IP	Peer IP address.
Peer Port	Peer port number.
State	Tunnel state.
Mac Address	AP MAC address, only displayed on ACs.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.41 show capwap statistics

Use this command to display statistics about the CAPWAP tunnel packets.

show capwap [*index* | [*ip-address* [*port*]]] **statistics**

Parameter Description

Parameter	Description
index	Tunnel index.
ip-address	Tunnel IP address.
port	Tunnel port number.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays packet statistics about the CAPWAP tunnel whose IP address is 1.1.1.1.

```
FS#show capwap 1.1.1.1 statistics
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.42 show version

Use this command to display the AP version.

show version { **all** | *ap-name* }

Parameter Description

Parameter	Description
all	All APs.
ap-name	Specifies an AP.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the version information on all APs.

```
FS#show version all
AP(AP220E-0)'s version:
    Product ID                    : AP220-E
    System uptime                 : 0:3:9:32
    Hardware version              : 2.00
    Software version              : AP_FSOS 11.1(2)B1
    Patch number                  : SP2
    Software number               : M05563609152014
    Serial number                 : 1234942570005
    MAC address                   : 00d0.f822.33b0

AP(AP220E-2)'s version:
    Product ID                    : AP220-E
    System uptime                 : 0:6:11:53
    Hardware version              : 2.00
    Software version              : AP_FSOS 11.1(2)B1
    Patch number                  : SP2
    Software number               : M05563609152014
    Serial number                 : 1234942570018
    MAC address                   : 001a.a9bd.0c1b
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.43 timestamp

Use this command to configure a specified AP or all APs in a specified AP group to synchronize with the AC in time.

timestamp

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode AP configuration mode/AP group configuration mode

Usage Guide N/A

Configuration Examples

The following example configures AP0001 to synchronize with the AC in time.

```
FS(config)# ap-config AP0001
FS(config-ap)# timestamp
```

The following example configures all APs in the AP group (Default) to synchronize with the AC in time.

```
FS(config)# ap-group default
FS(config-ap-group)# timestamp
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.44 tran-data-show

Use this command to display log information transmitted recently from a specified AP to the AC.

tran-data-show *ap-name* { **exception | cpuinfo | memory | syslog** | **tech-support** }

Parameter Description

Parameter	Description
ap-name	Indicates the name of the specified AP.
exception	Indicates the crash log information of the specified AP.

cpuinfo	Indicates the CPU information of the specified AP.
memory	Indicates the memory information of the specified AP.
syslog	Indicates the general log information of the specified AP.
tech-support	Indicates the console information of the specified AP.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example displays the crash log of AP0001.

```
FS(config-ac)# tran-data-show AP0001 exception
```

The following example displays the CPU information of AP0001.

```
FS(config-ac)# tran-data-show AP0001 cpuinfo
```

The following example displays the memory information of AP0001.

```
FS(config-ac)# tran-data-show AP0001 memory
```

The following example displays the general log information of AP0001.

```
FS(config-ac)# tran-data-show AP0001 syslog
```

The following example displays the console information of AP0001.

```
FS(config-ac)# tran-data-show AP0001 tech-support
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.45 tran-data-start

Use this command to obtain log information about a specified AP.

tran-data-start *ap-name* { **exception** | **memory** | **tech-support** | **tech-package** }

Parameter Description

Parameter	Description
ap-name	Indicates the name of the specified AP.
exception	Indicates the crash log information sent by the specified AP.
memory	Indicates the device status information sent by the specified AP, including CPU information, memory information, and general log information (including port UP/DOWN information).
tech-support	Indicates the console information.

tech-package	Indicates the package information.

Defaults N/A

Command Mode AC configuration mode

Usage Guide N/A

Configuration Examples

The following example obtains the crash log information from AP0001, and saves it as ap_AP0001_exception.log in the AC file system.

```
FS(config-ac)# tran-data-start AP0001 exception
```

The following example obtains the general log information from AP0001, and saves it as ap_AP0001_syslog.log, ap_AP0001_memory.log, and ap_AP0001_cpuinfo.log in the AC file system.

```
FS(config-ac)# tran-data-start AP0001 memory
```

The following example obtains the console information from AP0001, and saves it as ap_AP0001_8832.0000.1111_tech-console.log in the AC file system.

```
FS(config-ac)# tran-data-start AP0001 tech-support
```

The following example obtains the package information from AP0001, and saves it as ap_AP0001_8832.0000.1111_tech-package.tar.gz in the AC file system.

```
FS(config-ac)# tran-data-start AP0001 tech-package
```

Related Commands

Command	**Description**
N/A	N/A

Platform Description N/A

3.46 wired-interface

Use this command to enable the wired network port on the AP. Use the **no** form of this command to disable the wired port. Use the **default** form of this command to restore the default setting.

wired-interface [**port** *port-id*] **enable**

no wired-interface [**port** *port-id*] **enable**

default wired-interface [**port** *port-id*] **enable**

Parameter Description

Parameter	**Description**
port	Configures the wired network port.
port-id	Specifies the wired network port number, in the range from 1 to 4.
enable	Enables the wired network port.

Defaults

The wired network port is enabled by default.

Command Mode

AP configuration mode/ AP group configuration mode

Usage Guide

1. This command can be configured on all APs, but it takes effect only on the APs with wired network port.
2. If this command involves no port configuration, all wired network ports share the same configuration; if the four ports are disabled, no port configuration is displayed.
3. The fit AP obtains its configuration from the AC. The AP saves the wired port configuration automatically. When disconnected from the AC, the AP can restore the configuration after restart. If the wired port is disabled through configuration, the port remains disabled even after AP restart.

⚠ If the wired port on the AP is disabled, you cannot manage the AP through the wired port even after AP restart. It is recommended to long press the reset button on the AP to restore the factory setting.

Configuration Examples

The following example disables the wired network port on AP1.

```
FS(config)# ap-config AP1
FS(config-ap)# no wired-interface
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

3.47 wired-vlan

Use this command to configure the VLAN for the for the wired network port on the AP. Use the **no** form of this command to restore the default setting.

wired-vlan *vlan-id* [**port** *port-id*] **auto-save**

no wired-vlan [*vlan-id* [**port** *port-id*]] **auto-save**

Parameter Description

Parameter	Description
vlan-id	Specifies the VLAN where the wired network port resides, in the range from 1 to 4094.
port	Configures the wired network port.
port-id	Specifies the wired network port number, in the range from 1 to 4.
auto-save	Saves the configuration. The AP restores the configuration after restart.

Defaults

The wired network port and the AP are in the same VLAN by default.

Command Mode AP configuration mode/ AP group configuration mode

Usage Guide

1. This command can be configured on all APs, but it takes effect only on the APs with wired network port.
2. If this command involves no port configuration, all wired network ports are in the same VLAN; if the four ports are configured in the same VLAN, no port configuration is displayed.
3. In access AP mode (the AP does not assign IP addresses), when the wired network port and the AP are configured in the same VLAN, the VLAN where the wired network port resides is determined by the access switch rather than by this configuration. If the packet on the wired network port should be tagged, the Native VLAN of the access switch must be different from the VLAN where the wired network port resides. Otherwise, the packet cannot be forwarded to the wired network port.
4. In wireless routing mode (the AP assigns IP addresses), wired users obtain IP addresses from the DHCP address pool on the AP. The VLAN where the address pool interface resides must be consistent with the VLAN specified in this command.
5. The fit AP obtains its configuration from the AC. The **auto-same** parameter enables the AP to save the wired port configuration automatically. When disconnected from the AC, the AP can restore the configuration after restart to enable users to access the network through wired network port.

⚠ When the wired network port is enabled with the **auto-same** function and the VLAN where the wired network port resides is different from the Native VLAN of the AP, the AP cannot obtain the IP address after restart. It is recommended to long press the reset button on the AP to restore the factory setting.

Configuration Examples The following example configures VLAN 20 for the wired network port on AP1.

```
FS(config)# ap-config AP1
FS(config-ap)# wired-vlan 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4 WBS Commands

4.1 11asuport enable

Use the command to enable the specified radio to support 802.11a on 5 GHz. Use the **no** form of this command to disable the radio to support 802.11a on 5 GHz.

11asupport enable radio *radio-id*

no 11asupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, 802.11a is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11a on 5 GHz.

```
FS(config)# ap-config AP0001
FS(config-ap)# 11asupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.2 11bsupport enable

Use the command to enable the specified radio to support 802.11b on 2.4 GHz. Use the **no** form of this command to disable the radio to support 802.11b on 2.4 GHz.

11bsupport enable radio *radio-id*

no 11bsupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, 802.11b is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11b on 2.4 GHz.

```
FS(config)# ap-config AP0001
FS(config-ap)# 11bsupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.3 11gsupport enable

Use this command to enable the specified radio to support 802.11g on 2.4 GHz. Use the **no** form of this command to disable the radio to support 802.11g on 2.4 GHz.

11gsupport enable radio *radio-id*

no 11gsupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, 802.11g is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11g on 2.4 GHz.

```
FS(config)# ap-config AP0001
FS(config-ap)# 11gsupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.4 11nasupport enable

Use this command to enable the specified radio to support 802.11n on 5 GHz. Use the **no** form of this command to disable the radio to support 802.11n on 5 GHz.

11nasupport enable radio *radio-id*

no 11nasupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, 802.11n is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables radio1 to support 802.11n on 5 GHz.

```
FS(config)# ap-config AP0001
FS(config-ap)# 11nasupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.5 11ngsupport enable

Use this command to enable the specified radio to support 802.11n on 2.4 GHz. Use the **no** form of this command to disable the radio to support 802.11n on 2.4 GHz.

11ngsupport enable radio *radio-id*

no 11ngsupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, 802.11n is supported.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example enables radio1 to support 802.11n on 2.4 GHz.

```
FS(config)# ap-config AP0001
FS(config-ap)# 11ngsupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.6 11acsupport enable

Use this command to enable the specified radio to support 802.11ac. Use the **no** form of this command to disable the radio to support 802.11ac.

11acsupport enable radio *radio-id*

no 11acsupport enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, 802.11ac is supported when the radio ID is even.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example enables radio1 to support 802.11ac.

```
FS(config)# ap-config AP0001
FS(config-ap)# 11acsupport enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.7 802.11a network rate

Use this command to configure a RF rate list for the 802.11anetwork.

802.11a network rate { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }

Parameter Description

Parameter	Description
6	Indicates 6Mbps rate.
9	Indicates 9Mbps rate.
12	Indicates 12Mbps rate.
18	Indicates 18Mbps rate.
24	Indicates 24Mbps rate.
36	Indicates 36Mbps rate.
48	Indicates 48Mbps rate.
54	Indicates 54Mbps rate.
disabled	Not supported
mandatory	Supported
supported	Optional

Defaults

By default, the default value varies with the modes of the AP. For the 802.11a networks, the rates of 6, 12 and 24 are mandatory, and all others are supported.

Command Mode

AC configuration mode/AP configuration mode/AP group configuration mode

Usage Guide

None

Configuration Examples

The following example disables 6Mbps for 802.11a users.

```
FS(config)# ac-controller
FS(config-ac)# 802.11a network rate 6 disabled
```

The following example disables 6Mbps for 802.11a users on AP001.

```
FS(config)# ap-config AP001
FS(config-ap)# 802.11a network rate 6 disabled
```

The following example disables 6Mbps for 802.11a users on default group.

```
FS(config)# ap-group default
FS(config-group)# 802.11a network rate 6 disabled
```

Related Commands

Command	Description
-	-

Platform Description

N/A

4.8 802.11b network rate

Use this command to configure a RF rate list for the 802.11b network.

802.11b network rate { **1** | **2** | **5** | **11** } { **disabled** | **mandatory** | **supported** }

Parameter Description

Parameter	Description
1	Indicates 1Mbps rate.
2	Indicates 2Mbps rate.
5	Indicates 5Mbps rate.
11	Indicates 11Mbps rate.
disabled	Not supported
mandatory	Supported
supported	Optional

Defaults By default, 1Mbps, 2Mbps, 5.5Mbps, 11Mbps are mandatory.

Command Mode AC configuration mode/AP configuration mode/AP group configuraiton mode

Usage Guide None

Configuration Examples

The following example disables 1Mbps for 802.11b users.

```
FS(config)# ac-controller
FS(config-ac)# 802.11b network rate 1 disabled
```

The following example disables 1Mbps for 802.11b users on AP0001.

```
FS(config)# ap-config AP001
FS(config-ap)# 802.11b network rate 1 disabled
```

The following example disables 1Mbps for 802.11b users on default group.

```
FS(config)# ap-group default
FS(config-group)# 802.11b network rate 1 disabled
```

4.9 802.11g network rate

Use this command to configure a RF rate list for the 802.11g network.

802.11g network rate { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }

Parameter Description

Parameter	Description
1	Indicates 1Mbps rate.
2	Indicates 2Mbps rate.
5	Indicates 5Mbps rate.
6	Indicates 6Mbps rate.

9	Indicates 9Mbps rate.
11	Indicates 11Mbps rate.
12	Indicates 12Mbps rate.
18	Indicates 18Mbps rate.
24	Indicates 24Mbps rate.
36	Indicates 36Mbps rate.
48	Indicates 48Mbps rate.
54	Indicates 54Mbps rate.
disabled	Not supported
mandatory	Supported
supported	Optional

Defaults By default, 1Mbps, 2Mbps, 5.5Mbps, 11Mbps are mandatory. The others are optional.

Command Mode AC configuration mode/AP configuration mode/AP group configuration mode

Usage Guide None

Configuration Examples

The following example disables 1Mbps for 802.11g users..

```
FS(config)# ac-controller
FS(config-ac)# 802.11g network rate 1 disabled
```

The following example disables 1Mbps for 802.11g users on AP0001.

```
FS(config)# ap-config AP001
FS(config-ap)# 802.11b network rate 1 disabled
```

The following example disables 1Mbps for 802.11g users on default group.

```
FS(config)# ap-group default
FS(config-group)# 802.11b network rate 1 disabled
```

4.10 {802.11a | 802.11b} network [disable | enable]

Use this command to configure whether to enable or disable the 2.4GHz or 5GHZ network. When the 2.4GHz or 5GHZ network is disabled, all the wireless users connected with this wireless network will go offline.

{ **802.11a** | **802.11b** } **network** [**disable** | **enable**]

Parameter Description

Parameter	Description
N/A	N/A

Defaults The default is **enable**.

Command Mode ac configuration mode.

Usage Guide None

Configuration Examples

Example 1: Configure the 802.11a network disable

```
FS(config-ac)# 802.11a network disable
```

Related Commands

Command	Description
-	-

Platform Description N/A

4.11 80.211n a-mpdu enable

Use this command to enable the specified radio to support AMPDU. Use the **no** form of this command to disable the radio to support AMPDU.

802.11n a-mpdu enable radio *radio-id*

no 802.11n a-mpdu enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults AMPDU is enabled by default.

Command mode AP configuration mode

Usage Guide This command takes effect only when the radio operates in 802.11n or 802.11ac,

Configuration Examples

The following example enables radio1 to support AMPDU.

```
FS(config)# ap-config AP0001
FS(config-ap)# 802.11n a-mpdu enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.12 80.211n mcs support

Use this command to configure the modulation and coding scheme (MCS) index of 802.11n. Use the **no** form of this command to restore the default MCS of 802.11n.

802.11n mcs support *num* **radio** *radio-id*

no 802.11n mcs support radio *radio-id*

Parameter Description

Parameter	Description
num	MCS index. The range is from 0 to 31.
radio-id	Radio ID. The range is from 1 to 96.

Defaults

The default MCS index of 802.11n is 31.

Command mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the MCS index to 15 of 802.11n for radio1.

```
FS(config)# ap-config AP0001
FS(config-ap)# 802.11n mcs support 15 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.13 80.211ac mcs support

Use this command to configure the modulation and coding scheme (MCS) index of 802.11ac. Use the **no** form of this command to restore the default MCS of 802.11ac.

802.11ac mcs support *num* **radio** *radio-id*

no 802.11ac mcs support radio *radio-id*

Parameter Description

Parameter	Description
num	MCS index. The range is from 0 to 39.
radio-id	Radio ID. The range is from 1 to 48.

Defaults

The default MCS index of 802.11ac is 39.

Command mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the MCS index to 19 of 802.11ac for radio1.

```
FS(config)# ap-config AP0001
FS(config-ap)# 802.11ac mcs support 19 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.14 ampdu-retries

In a wireless network, AMPDU software retransmission is adopted to reduce the sub-frame loss. The more retransmission attempts, the less the package loss. However excessive retransmission attempts increase the workload of air interfaces, which reduce the immediacy of other packages. So, it is recommended to configure more retransmission attempts when sub-frame loss frequently occurs.

ampdu-retries *times* **radio** *radio_id*

Parameter Description

Parameter	Description
times	Retransmission times. The range is from 1 to 10.
radio-id	Radio ID. The range is from 1 to 48.

Defaults

By default, the retransmission times is 10.

Command Mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example enters the configuration mode of AP0001 and sets the AMPDU software retransmission times to 2.

```
FS(config)#ap-config AP0001
FSe(config-ap)#ampdu-retries 2 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.15 ampdu-rts

Use this command to enable the Request to Send (RTS) protection mode for the AMPDU packets.

Use the **no** form of this command to disable the RTS mode.

ampdu-rts radio { *radio-id* | *802.11b* | *802.11a*] }

no ampdu-rts radio { *radio-id* | *802.11b* | *802.11a*] }

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults This function is disabled by default.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example enters the configuration mode of AP0001 and enables the AMPDU RTS protection on the radio 1.

```
FS(config)# ap- config AP0001
FS(config-ap)# ampdu-rts radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.16 antdetect enable

Use this command to enable extension cable link detection function. Use the **no** form of this command to restore to disable extension cable detection.

antdetect enable

no antdetect enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults Extension cable detection is disabled by default.

Command Mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables i-Share antenna extension cable link detection function:

```
FS(config-ap)#antdetect enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.17 antdetect interval

Use this command to configure the time interval of the extension cable link detection. Use the **no** form of this command to restore the default detection interval.

antdetect interval *interval*

no antdetect interval

Parameter Description

Parameter	Description
interval	Indicates the detection interval. The unit is minute, and the range is from 1 to 10,000.

Defaults

The default detection interval is 1 minute.

Command Mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the time interval of detection as 1 minute:

```
FS(config-ap)#antdetect enable
FS(config-ap)#antdetect interval 1
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

4.18 antenna receive

Use this command to configure the receiving antenna type of the specified radio for the specified AP or all APs of the specified AP group.

antenna receive *value* **radio** *radio-id*

Parameter Description

Parameter	Description
value	Antenna mask. The range is from 1 to 15.
radio-id	Radio ID. The range is from 1 to 48.

Defaults

For AP configuration mode, the default receiving antenna type depends on device model.

For AP group configuration mode, there is no default setting.

Command Mode

AP configuration mode/AP group configuration mode

Usage Guide

This command takes effect only on the AP device operating in 802.11n.

Configuration Examples

The following example configures the receiving antenna type to 5 for AP001.

```
FS(config)# ap-config AP0001
FS(config-ap)# antenna receive 5 radio 1
```

The following example configures the receiving antenna type to 5 for AP group.

```
FS(config)# ap-group default
FS(config-group)# antenna receive 5 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.19 antenna transmit

Use this command to configure the transmitting antenna type of the specified radio or all APs of the specified AP group..

antenna transmit *value* **radio** *radio-id*

Parameter Description

Parameter	Description
value	Antenna mask. The range is from 1 to 15.
radio-id	Radio ID. The range is from 1 to 48.

Defaults For AP configuration mode, the default receiving antenna type depends on device model.

For AP group configuration mode, there is no default setting.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide This command takes effect only on the AP device operating in 802.11n.

Configuration Examples The following example configures the transmitting antenna type to 7 on AP001.

```
FS(config)# ap-config AP0001
FS(config-ap)# antenna transmit 7 radio 1
```

The following example configures the transmitting antenna type to 7 on the AP group (default).

```
FS(config)# ap-group default
FS(config-group)# antenna transmit 7 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.20 apsd

Use this command to enable the unscheduled-automatic power save delivery (U-APSD) mode for the specified radio of an AP device.

apsd { **enable** | **disable** } **radio** *radio-id*

Parameter Description

Parameter	Description
enable	Enables the U-APSD mode.
disable	Disables the U-APSD mode.
radio-id	Radio ID. The range is from 1 to 48.

Defaults U-APSD mode is enabled by default.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the U-APSD mode for radio1.

```
FS(config)# ap-config AP0001
FS(config-ap)#apsd enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.21 autowifi

Use this command to enable one-click WLAN configuration on an unconfigured device. Use the **no** form of this command to remove the one-click WLAN configuration.

autowifi

no autowifi

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

AC global configuration mode

Usage Guide

One-click WLAN configuration function is provided for fast configuration on an unconfigured device,

⚠ In general, this function aims at helping the scenario investigator to improve efficiency and helping the channel distributors to test WLAN performance in a more convenient way.

Configuration Examples

The following example configures one-click WLAN configuration.

```
FS(config)# autowifi
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.22 assoc-rssi

Use this command to configure the minimum RSSI for the STA to associate with the specified AP. Use the **no** form of this command to restore the default setting.

response-rssi *rssi* **radio** *radio-id*

no response-rssi radio *radio-id*

Parameter Description

Parameter	Description
rssi	Specifies the RSSI. The range is from 0 to 100. The unit is dBm.
radio-id	Radio ID. The range is from 1 to 48.

Defaults

The default RSSI is 0, namely, the STA any RSSI can associate with the AP.

Command mode

AP configuration mode

Usage Guide

This command is used to clear sticky STAs in roaming scenario, It is recommended to set RSSI to a value in the range from 15 to 30.

Configuration Examples

The following example enters AP0001 configuration mode and sets the minimum RSSI for the STA to associate with AP0001 to 15.

```
FS(config)# ap-config AP0001
FS(config-ap)# assoc-rssi 15 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.23 beacon dtim-period

Use this command to configure the period of delivery transmission indication messages (DTIM) for the specified radio.

beacon dtim-period *period-num* **radio** *radio-id*

Parameter Description

Parameter	Description
period-num	DTIM period, which indicating the beacon periods. The range is from 1 to 255.
radio-id	Radio ID. The range is from 1 to 48.

Defaults

The default DTIM period is 1 (namely, 1 beacon period).

Command Mode

AP configuration mode.

Usage Guide

N/A

Configuration Examples

The following example configures the DTIM period of radio 1 of AP0001 to 30 beacon periods.

```
FS(config)# ap-config AP0001
FS(config-ap)# beacon dtim-period 30 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.24 beacon period

Use this command to configure the beacon period forthe specified radio of the specified AP.

beacon period *milliseconds* **radio** *radio-id*

Parameter Description

Parameter	Description
milliseconds	Beacon period. The range is from 20 to 1,000. The unit is millisecond.
radio-id	Radio ID. The range is from 1 to 48.

Defaults

The default is beacon period is 100 milliseconds.

Command Mode

AP configuration mode.

Usage Guide

N/A

Configuration Examples

The following example configures the beacon period of radio 1 of AP0001 to 200 milliseconds.

```
FS(config)# ap-config AP0001
FS(config-ap)# beacon period 200 radio 1
```

Related Commands

Command	Description
-	-

Platform Description

N/A

4.25 beacon rate

Use this command to configure the beacon rate for the specified radio. Use the **no** form of this command to restore the default beacon rate.

beacon rate *rate-Mbps* **radio** { *radio-id* | *802.11b* | *802.11a*] }

no beacon rate radio { *radio-id* | *802.11b* | *802.11a*] }

Parameter Description

Parameter	Description

rate-Mbps	Specifies the beacon rate. 1, The rate blocked in the rate set cannot be set as a beacon rate. 2. The rates of 1Mbps, 2Mbps, 5.5Mbps and 11 Mbps are not supported by the radios on 5 GHz.
radio-id	Radio ID. The range is from 1 to 48.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults

No beacon rate is configured by default.

Command mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the beacon rate of radio1 to 12Mbps.

```
FS(config)# ap-config AP0001
FS(config-ap)# beacon rate 12.0 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.26 chan-width

Use this command to set the bandwidth of the specified radio.

chan-width { **20** | **40** | **80** | **160** } **radio** { *radio-id* | *802.11b* | *802.11a*] }

Parameter Description

Parameter	Description
20	Sets the radio width to 20 Mbps.
40	Sets the radio width to 40 Mbps.
80	Sets the radio width to 80 Mbps.
160	Sets the radio width to 160 Mbps.
radio-id	Sets radio ID. The range is from 1 to 48.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults

The default channel bandwidth of 20 Mbps.

Command mode AP configuration mode

Usage Guide The radio bandwidth configuration takes effect only for the AP device operating at 802.11n mode.

Configuration Examples The following example sets the radio width of radio1 to 40 Mbps.

```
FS(config)# ap-config AP0001
FS(config-ap)# chan-width 40 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.27 channel

Use this command to configure a channel for the specified radio of the specified AP.

channel { **global** | *channel-id* } **radio** *radio-id*

Parameter Description

Parameter	Description
chan-id	Specifies the channel ID.
global	Indicates that the channel is specified through the radio resource management (RRM) function.
radio-id	Sets radio ID. The range is from 1 to 48.

Defaults By default, the **global** parameter is used.

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples The following example specifies channel 6 for radio 1.

```
FS(config)# ap-config AP0001
FS(config-ap)# channel 6 radio 1
```

Related Commands

Command	Description
-	-

Platform Description N/A

4.28 country

Use this command to specify a country code for an AC device. Use the **no** form of this command to remove the country code settings for an AC device.

country *country-code*

no country *country-code*

Use this command to specify a country code for the specified radio of an AP device.

country *country-code* **radio** { *radio-id* | [*802.11b* | *802.11a*] }

Parameter Description

Parameter	Description
country-code	Country code.
radio-id	Sets radio ID. The range is from 1 to 48.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults

By default, the country code supported by an AC device is **CN**, and the country code used by an AP device is **CN**.

Command Mode

AC/AP configuration mode.

Usage Guide

1. The country code "CN" supported by an AC cannot be deleted.
2. This command cannot be configured for all APs at the same time.
3. 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.
4. Before configuring a country code for an AP, add the country code to the country code set supported by the AC. If the country code used by an AP changes, the radio band, channel, and power of the AP change accordingly.
5. If **802.11b** is specified, the country code is configured for all 2.4 GHz radios; the configuration takes effect when the AP goes online for the first time, and it takes effect on the specified radios only. When **802.11a** is specified, the country code is configured for all 5.8 GHz radios; the configuration takes effect when the AP goes online for the first time and it takes effect on the specified radios only.
6.

Configuration Examples

The following example configures a country code supported by an AC device to US.

```
FS(config)# ac-controller
FS(config- ac)# country US
FS(config- ac)# exit
```

The following example configures a country code for radio 1 of AP0001 to US.

```
FS(config)# ap-config AP0001
FS(config-ap)# country US radio 1
```

Related Commands

Command	Description
-	-

Platform Description

N/A

4.29 coverage-area-control

Use this command to set the coverage area control power. Use the **no** form of this command to restore the default coverage area control power.

coverage-area-control *power*

no coverage-area-control

Parameter Description

Parameter	Description
power	Specifies the coverage area control power. The unit is dBm. The range is from 0 to 32.

Defaults

The default value is 0.

Command mode

AP configuration mode/AP group configuration mode

Usage Guide

N/A

Configuration Examples

The following example enters AP0001 configuration mode and sets the coverage area control power to 20.

```
FS(config)# ap-config AP0001
FS(config-ap)# coverage-area-control 20
```

The following example enters AP group configuration mode and sets the coverage area control power to 20.

```
FS(config)# ap-group default
FS(config-group)# coverage-area-control 20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.30 ebag

Use this command to enable ebag network optimization. Use the **no** form of this command to disable ebag network optimization.

ebag

no ebag

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

AP configuration mode

Usage Guide

This command is generally used in e-bag scenario. Use this function with caution in other scenarios.

Configuration Examples

The following example enables ebag network optimization.

```
FS(config)# ap-config AP0001
FS(config-ap)# ebag
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.31 enable-radio

Use this command to enable a/all radio for an AP device. Use the **no** form of this command to disable a/all radios.

enable-radio { *radio-id* | **all** }

no enable-radio { *radio-id* | **all** }

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.
all	Enables all radios.

Defaults

By default, all radios of the AP device are enabled.

Command Mode

AP configuration mode.

Usage Guide

Note:

This operation may result in offline of all the wireless users connected to the specified radio.

Configuration Examples

The following example enters the configuration mode of AP0001 and disables radio 1.

```
FS(config)# ap- config AP0001
FS(config-ap)# no enable-radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.32 eth-schd

Use this command to configure maximum number of Ethernet packets received on the AP device for one time. Use the **no** form of this command to restore the default number of packets received for one time.

eth-schd *limit*

no eth-schd

Parameter Description

Parameter	Description
limit	The maximum number of Ethernet packets received for one time. The range is from 1 to 256.

Defaults

The default limit value varies by AP model.

Command Mode

AP configuration mode

Usage Guide

You can improve the network performance by raising the received Ethernet packets limit for every time on an AP, at the cost of reducing immediacy of packets of key services. With regard to applications which are multi-user concurrent and real-time sensitive, such as electronic schoolbag, requiring only ordinary networks, you are recommended to decrease the value of received Ethernet packets limit per time to 25.

Configuration Examples

The following example enters the configuration mode of AP0001 and sets the maximum number of the Ethernet packets received per time to 50.

```
FS(config)# ap- config AP0001
FS(config-ap)# eth-schd 50
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.33 external-antenna enable

Use this command to enable the external antenna and disable the built-in antenna on the AP device.

external-antenna enable radio *radio-id*

no external-antenna enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Specifies the radio ID in the range from 1 to 48.

Defaults By default, the built-in antenna is enabled, and the external antenna is disabled.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enables the external antenna and disables the built-in antenna on AP001.

```
FS(config)# ap-config AP0001
FS(config-ap)# external-antenna enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.34 fragment-threshold

Use this command to set a fragment threshold for a radio. Use the **no** form of this command to restore the default fragment threshold.

fragment-threshold *value* **radio** *radio-id*

no fragment-threshold radio *radio-id*

Parameter Description

Parameter	Description
value	Specifies the fragment threshold. The value is an even number ranging from 256 to 2.346.
radio-id	Radio ID. The range is from 1 to 48.

Defaults The default fragment threshold is 2,346.

Command AP configuration mode

mode

Usage Guide N/A

Configuration Examples The following example sets the fragment threshold of radio1 to 1,538.

```
FS(config)# ap-config AP0001
FS(config-ap)# fragment-threshold 1538   radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.35 green-field enable

Use this command to enable the green-field protection mode for the specified radio. Use the **no** form of this command to disable the green-field protection mode.

green-field enable radio *radio-id*

no green-field enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, the green-field protection mode is disabled.

Command mode AP configuration mode

Usage Guide This command is supported only for the radio on 2.4 GHz.

Configuration Examples The following example enables the green-field protection mode for radio1.

```
FS(config)# ap-config AP0001
FS(config-ap)# green-field enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.36 ldpc

Use this command to enable low density parity check (LDPC) coding for the specified radio. Use the **no** form of this command to disable LDPC coding.

ldpc radio *radio-id*

no ldpc radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, LDPC coding is enabled.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example enters the configuration mode of AP0001 and enables LDPC coding on radio 1.

```
FS(config)# ap-config AP0001
FS(config-ap)# ldpc radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.37 link-check

Use this command to enable/disable link check.. Use the **no** form of this command to restore the default setting.

link-check { **enable** | **disable** }

no link-check { **enable** | **disable** }

Parameter Description

Parameter	Description
enable	Enables link check.
disable	Disables link check.

Defaults Link check is disabled by default.

Command mode Global configuration mode

Usage Guide N/A

Configuration Examples

The following example enables link check.

```
FS(config)# link-check enable
```

The following example disables link check.

```
FS(config)# link-check disable
```

or

```
FS(config)# no link-check enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.38 linktest

Use this command to display the link information about a wireless client.

linktest *H.H.H*

Parameter Description

Parameter	Description
H.H.H	MAC address of the wireless client.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the link information about a wireless client.

```
FS# linktest cca2.2352.768d
Link test station(cca2.2352.768d):
    Signal strength in the form of RSSI :                  55
    Signal quality in the form of SNR:                      -37
    Total number of packets that are retried:            9
    Maximum retry count for a single packet:              16
    Number of lost packets:                                    0
    Data rate of a successfully transmitted packet: 0
```

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

4.39 mcast-rate

Use this command to configure the multicast rate for WLAN. Use the **no** form of this command to restore the default multicast rate of WLAN.

mcast-rate *mcast-num*

no mcast-rate

Parameter Description

Parameter	Description
mcast-num	WLAN multicast rate. The available rates: 1Mbps, 6Mbps, 11Mbps, 24Mbps, 54Mbps.

Defaults The default WLAN multicast rate is 24Mbps.

Command mode WLAN configuration mode

Usage Guide N/A

Configuration Examples The following example configures the multicast rate of WLAN2048 to 11Mbps.

```
FS(config)# wlan-config 2048
FS(config-wlan)# mcast-rate 11
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.40 mu-mimo enable

Use this command to enable MU-MIMO for the specified radio. Use the **no** or **default** form of this command to restore the default setting.

mu-mimo enable radio *radio-id*

no mu-mimo enable radio *radio-id*

default mu-mimo enable radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Specifies a radio, in the range from 1 to 48.

Defaults

If the specified radio does not support MU-MIMO, MU-MIMO is disabled by default. If the radio supports MU-MIMO and it is enabled on the radio by default, it is enabled on the AC by default. If the radio supports MU-MIMO and it is disabled on the radio by default, it is disabled on the AC by default.

Command Mode

AP configuration mode/ All-AP configuration mode/AP group configuration mode

Usage Guide

Configuration Examples

The following example enters AP0001 configuration mode and enable MU-MIMO for radio1.

```
FS(config)# ap-config AP0001
FS(config-ap)# mu-mimo enable radio 1
```

The following example enters AP0001 configuration mode and disables MU-MIMO for radio2.

```
FS(config)# ap-config AP0001
FS(config-ap)# no mu-mimo enable radio 2
```

The following example enters AP0001 configuration mode and restores MU-MIMO setting for radio3.

```
FS(config)# ap-config AP0001
FS(config-ap)# default mu-mimo enable radio 3
```

The following example enters All-AP configuration mode and enables MU-MIMO for radio1.

```
FS(config)# ap-config all
FS(config-ap)# mu-mimo enable radio 1
```

The following example enters default configuration mode and enables MU-MIMO for radio1.

```
FS(config)# ap-group default
FS(config-group)# mu-mimo enable radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.41 peer-distance

Use this command to configure the maximum distance between the specified radio and the peer.

peer-distance *val* **radio** *radio-id*

Parameter Description

Parameter	Description
val	The maximum distance between the radio and the peer. The range is from

	1,000 to 25,000. The unit is meter.
radio-id	Radio ID. The range is from 1 to 48.

Defaults The default distance between the radio and the peer is 1,000 meters.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example configures the maximum distance between radio and the peer to 3,000 meters.

```
FS(config)# ap-config AP0001
FS(config-ap)# peer-distance 3000 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.42 power local

Use this command to configure trasmit power for the specified radio of the specified AP.

power local { **global** | *power* } **radio** { *radio-id* | [*802.11b* | *802.11a*] }

Parameter Description

Parameter	Description
power	Indicates the percentage of transmit power. The range is from 1 to 100.
Global	Indicates that the transmit power is specified through RRM for the specified AP or all APs of the specified AP group.
radio-id	Radio ID. The range is from 1 to 48.
802.11b	Configures 2.4GHz radio.
802.11a	Configures 5.8GHz radio.

Defaults By default, the **global** parameter is used.

Command Mode AP configuration mode/AP group configuration mode

Usage Guide N/A

Configuration Examples

The following example configures the transmit power of radio1 of AP0001 to 50%.

```
FS(config)# ap-config AP0001
FS(config-ap)# power local 50 radio 1
```

The following example configures the transmit power of radio 1 of AP group (default) to 50%.

```
FS(config)# ap-group default
FS(config-group)# power local 50 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.43 preamable

Use this command configure the preamable attribute for the specified radio of the specified AP.

preamable { **long** | **short** } **radio** *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.
long	Indicates that the AP transmits only frames of long preamable.
short	Indicates that the AP transmits frames of short or long preamable.

Defaults

By default, is **short** parameter is used.

Command Mode

AP configuration mode.

Usage Guide

N/A

Configuration Examples

The following example configures the preamable attribute of radio 1 of AP0001 to **long**.

```
FS(config)# ap-config AP0001
FS(config-ap)# preamable long radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.44 radio-type

Use this command to configure the RF mode for the specified radio of the specified AP.

radio-type *radio-id* {**802.11a | 802.11b**}

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.
802.11a	Indicates the 5GHz band is used.
802.11b	Indicates the 2.4GHz band is used.

Defaults By default, the AP device with single radio (namely, radio1) operates in 2.4 GHz, while the AP device with dual radios can operate in 2.4 GHz (radio1) and 5 GHz (radio2).

Command Mode AP configuration mode.

Usage Guide N/A

Configuration Examples The following example configures radio 1 of AP0001 to operates in 2.4 GHz.

```
FS(config)# ap-config AP0001
FS(config-ap)# radio-type 1 802.11a
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.45 response-rssi

Use this command to set the minimum received signal strength indication (RSSI) for wireless client to associate with the AP. Use the **no** form of this command to restore the default setting.

response-rssi *rssi* **radio** { *radio-id* | [*802.11b* | *802.11a*] }

no response-rssi radio { *radio-id* | [*802.11b* | *802.11a*] }

Parameter Description

Parameter	Description
rssi	Specifies the RSSI. The range is from 0 to 100. The unit is dBm.
radio-id	Radio ID. The range is from 1 to 48.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

Defaults The default RSSI is 0, namely, the wireless client of any RSSI can associate with the AP.

Command mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example configures the minimum access RSSI to 20.

```
FS(config)# ap-config AP0001
FS(config-ap)# response-rssi 20 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.46 rts-threshold

Use this command to configure the RTS threshold of the specified radio. Use the **no** form of this command to restore the default RTS threshold.

rts-threshold *value* **radio** *radio-id*

no rts-threshold radio *radio-id*

Parameter Description

Parameter	Description
value	RTS threshold. The unit is byte. The range is from 257 to 2,347.
radio-id	Radio ID. The range is from 1 to 48.

Defaults

The default RTS threshold is 2,347.

Command mode

AP configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the RTS threshold of radio1 to 1,539.

```
FS(config)# ap-config AP0001
FS(config-ap)# rts-threshold 1539 radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.47 short-gi

Use this command to enable the radio to support short-gi. Use the **no** form of this command to disable the radio to support short-gi.

short-gi enable radio *radio-id* **chan-width** { **20** | **40** | **80** |**160** }

no short-gi enable radio *radio-id* **chan-width** { **20** | **40** | **80** |**160** }

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.
20	Configures the channel bandwidth to 20 Mbps.
40	Configures the channel bandwidth to 40 Mbps.
80	Configures the channel bandwidth to 80 Mbps.
160	Configures the channel bandwitdth to 160 Mbps.

Defaults By default, 20Mbps, 40Mbps, 80Mbps and 160Mbps are enabled.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples

The following example enables radio1 to support the short-gi of 20Mbps.

```
FS(config)# ap-config AP0001
FS(config-ap)# short-gi enable radio 1 chan-width 20
```

The following example disables radio2 to support the short-gi of 40Mbps.

```
FS(config)#ap-config AP0001
FS(config-ap)# no short-gi enable radio 2 chan-width 40
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.48 short-slot-time

Use this command to enable short slot time for the AP device. Use the **no** form of this command to disable short slot time.

short-slot-time radio *radio-id*

no short-slot-time radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, short slot time is enabled on the AP device.

Command mode AP configuration mode

Usage Guide Short slot time takes effect only on the AP working in 5GHz.

Configuration Examples The following example enables short slot time on radio1.

```
FS(config)#ap-config AP0001
FS(config-ap)# short-slot-time radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.49 stbc

Use this command to enable space-time block code (STBC) for the specified radio. Use the **no** form of this command to disable STBC.

stbc radio *radio-id*

no stbc radio *radio-id*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.

Defaults By default, STBC is enabled.

Command Mode AP configuration mode

Usage Guide N/A

Configuration Examples The following example enters the configuration mode of AP0001 and enable STBC for radio1.

```
FS(config)# ap- config AP0001
FS(config-ap)# stbc radio 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.50 show ac-config { 802.11a | 802.11b } summary

Use this command to display the AP devices supporting in 802.11a/b on the AC device.

show ac-config { **802.11a** | **802.11b** } **summary**

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the AP devices supporting 802.11a on the AC device.

```
FS#show ac-config 802.11a summary
Index   Ap name                                         slot id    Radio Base MAC    state       load(%)
noise(dBm) interfere(%)
------ ---------------------------------------- -------- --------------- -------- -------- ---------- ---------------
1       ap320v1.0                                   2          0000.0000.0000    Enable    0          -110
0
2       00d0.fb88.7812                              2          00d0.fb88.7815    Enable    0          -110
0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.51 show antenna all

Use this command to display antenna status of all APs.

show antenna all

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command

Privileged EXEC Mode.

Mode

Usage Guide Use this command to display the antenna status.

Configuration Examples The following example displays the antenna status 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 -     - - - -     - - - -
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.52 show antenna single

Use this command to display antenna status of the specified AP.

show antenna single *ap-name*

Parameter Description

Parameter	Description
ap-name	AP device name.

Defaults N/A

Command Mode Privileged EXEC Mode.

Usage Guide Use this command to display the antenna status of the specified AP.

Configuration Examples The following example displays the antenna status of "APD-M4":

```
FS# show antenna single APD-M4
```

```
ap[APD-M4] antenna state
R1-1: N
```

```
R1-2: N

R2-1: N

R2-2: N

R3-1: N

R3-2: N

R4-1: N

R4-2: N
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.53 show ap-config radio

Use this command to display the radio configuration of all APs .

show ap-config radio

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the radio configuration of all AP devices.

```
FS#show ap-config radio
Show all AP radios:
AP Name                                   MAC Address          Radio MAC            Radio MAC
--------------------------------------- ------------------- ------------------- -------------------
AP0001                                    N/A                  N/A                  N/A
```

Field	Description
AP Name	AP Name
MAC Address	AP MAC address
Radio MAC	MAC address of odd Radio ID
Radio MAC	MAC address of even Radio ID

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.54 show ap-config radio ap-name

Use this command to display the radio configuration of all APs.

show ap-config radio ap-name *ap-name*

Parameter Description

Parameter	Description
ap-name	AP device name

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the radio configuration of all APs.

```
FS#show ap-config radio ap-name
Radio ID Radio Type        STA NUM   Channel   Power   Radio Base MAC    Status
-------- --------------- -------- -------- ------ --------------- -------
1            802.11b/g/n        10            6*             100       000c.3067.fbd7    Enable
2            802.11a/n/ac    0            149*          100       000c.3067.fbd8    Disable
```

Field	Description
Radio ID	RF port ID
Radio Type	Radio band
STA NUM	STA number
Channel	Channel
Power	Power
Radio Base MAC	MAC address of RF port
Status	RF port status

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.55 show ap-config radio config

Use this command to display the radio configuration of the specified AP.

show ap-config radio *radio-id* **config** *ap-name*

Parameter Description

Parameter	Description
ap-name	AP device name
radio-id	Radio ID. The range is from 1 to 48.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the radio configuration of the specified AP.

```
FS# show ap-config radio 1 config 220em
Admin State................................ Enable
Current Tx Power........................... Global
Num of BSSIDs.............................. 1
DTIM Period................................ 1
Beacon Period(milliseconds)................ 100
Country Code............................... CN
Current Channel............................ Global
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.56 show ap-config radio info

Use this command to display radio information of the specified AP.

show ap-config radio info *ap-name*

Parameter Description

Parameter	Description
ap-name	Specifies an AP

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays radio information of all APs.

```
FS#show ap-config radio info ap-name
Radio ID Radio Type      MU-MIMO        Radio Base MAC    Status
-------- ------------ ---------- -------------- -------
1             802.11b/g/n    Nonsupport 000c.3067.fbd7    Enable
2             802.11a/n/ac Enable         000c.3067.fbd8    Disable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.57 show ap-config radio radio-id status

Use this command to display details about the radio configuration of the specified AP device.

show ap-config radio *radio-id* **status** *ap-name*

Parameter Description

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.
ap-name	AP device name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays details about the radio configuration of the specified AP.

```
FS# show ap-config radio 1 s 220em
Admin State............................. Enable
Oper State.............................. Normal
WTP Radio Statistics
  Last Fail Type......................... Statistic Not Supported
  Reset Count............................ 0
  SW Failure Count....................... 0
  HW Failure Count....................... 0
  Other Failure Count................... 0
  Unknown Failure Count.................. 0
  Config Update Count................... 0
  Channel Change Count.................. 2
  Band Change Count..................... 197
  Current Noise Floor................... -102
Assigned WTP BSSID
  WLAN ID.............................. 0
  MAC Address........................... 0000.0000.0000
MIC Countermeasures
  WLAN ID.............................. 0
  MAC Address........................... 0000.0000.0000
RSNA Error Report From Station
  Client MAC Address.................... 0000.0000.0000
  Radio Base MAC........................ 0000.0000.0000
  Radio ID............................. 1
  WLAN ID.............................. 0
  TKIP ICV Errors....................... 0
  TKIP Local MIC Failures................ 0
  TKIP Remote MIC Failures............... 0
  CCMP Replays.......................... 0
  CCMP Decrypt Errors................... 0
  TKIP Replays.......................... 0
Statistics
  Tx Fragment Count..................... 0
  Multicast Tx Count.................... 0
  Failed Count.......................... 0
  Retry Count........................... 0
  Multiple Retry Count.................. 0
  Frame Duplicate Count.................. 0
  RTS Success Count..................... 0
  RTS Failure Count..................... 0
  ACK Failure Count..................... 0
  Rx Fragment Count..................... 0
  Multicast RX Count.................... 0
  FCS Error Count....................... 0
  Tx Frame Count ....................... 0
  Decryption Errors..................... 0
  Discarded QoS Fragment Count........... 0
  Associated Station Count............... 0
  QoS CF Polls Received Count............ 0
  QoS CF Polls Unused Count.............. 0
  QoS CF Polls Unusable Count............ 0
Current Tx Power....................... 100
Current Tx Power Value.................. 28
Tx Power Level Num...................... 0
WebAuth online sta Count.................0
DOT1x online sta Count...................0
Security sta Count.......................0
WTP Radio Fail Alarm Indication
  Type.................................. Unknown
  Status................................ 0
  Pad................................... 0
WTP Radio Information
Radio Type.............................. 802.11b
WTP Radio Config
  Short Preamble........................ 0
  Number of BSSIDs...................... 1
  DTIM Period........................... 0
  Radio Base MAC........................ 00d0.f822.33da
  Beacon Period(milliseconds)............ 100
  Country String........................ CNI
Direct Sequence Control
  Current Channel....................... 11
  Current CCA........................... 1
  Energy Detect Threshold................ 1
MAC Operation
  RTS Threshold......................... 2347
  Short Retry........................... 7
  Long Retry............................ 4
  Fragmentation Threshold................ 2346
  Tx MSDU Lifetime...................... 0
  Rx MSDU Lifetime...................... 0
Multi-Domain Capability
  First Channel......................... 0
  Number of Channels.................... 0
  Max Tx Power Level.................... 0
OFDM Control
  Current Channel....................... 0
  Band Supported........................ 0
  TI Threshold.......................... 0
Capability
  Power Default......................... 28
  Power Max............................. 28
  Power Min............................. 1
  Power Per Default..................... 100
  Power Per Max......................... 100
  Power Per Min......................... 4
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.58 show ap-config radio status

Use this command to display the radio list of an AP device.

show ap-config radio status *ap-name*

Parameter Description

Parameter	Description
ap-name	AP device name.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the radio list of the specified AP.

```
FS# show ap-config radio status 220em
Radio Slot    Radio Type         Sub Band     Admin Status       Oper Status        Regulary Domain          Radio
Base MAC
----------- --------------- ---------- --------------- --------------- -------------------- --------------------
1                  802.11b/g/n                -                Enable                -                       Supported
00d0.f822.33da
2                  802.11a/n                  -                Enable                -                       Supported
00d0.f822.33db
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.59 show ap-config summary radio

Use this command to display all APs on the specified radio.

show ap-config summary radio [*radio-id*]

Parameter

Parameter	Description

Description

radio-id	Specifies a radio, in the range from 1 to 48.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays all APs on radio 1.

```
FS#sh ap-config summary radio 1
Ap Name                                          Radio Base MAC    STA NUM    Radio Type AP IP
---------------------------------------- --------------- -------- ---------- ---------------
AP530-I1.01                                    0014.4b74.d427    0          802.11b       172.18.57.195
AP330-I1.1                                     0014.4b6d.e18f    8          802.11b       172.18.57.227
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.60 show client details

Use this command to display the information of the specified wireless client.

show client details *sta-mac*

Parameter Description

Parameter	Description
sta-mac	MAC address of the wireless client. The format is H.H.H.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the information of wireless client “0025.9c9b.aeb5”.

```
FS# show client details 0025.9c9b.aeb5
The Details of Client 0025.9c9b.aeb5:
     RSSI.................... 28
     SNR..................... -67
     AID..................... 1
```

```
RX Data................. 51
RX Management........... 0
RX Control.............. 0
RX Unicast.............. 25
RX Multicast............ 0
RX Bytes................ 6174
TX Data................. 3
TX Management........... 0
TX Unicast.............. 3
TX Multicast............ 0
TX Bytes................ 228
TX Probe................ 0
TX Assoc................ 0
TX Assoc Fail........... 0
TX Auth................. 0
TX Auth Fail............ 0
TX Deauth............... 0
TX Disassoc............. 0
Packet Load............. 51216
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.61 show smart bad radio

Use this command to display the bad radio on AP5280.

show smart bad radio

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the bad radio on AP5280.

Examples

```
AC#show smart bad radio

Ap-name                  ap-mac                 radio
-------------------      ---------------        ----------------

AP5280-1                 00d0.1234.4565         1,2,3,4,
AP5280-2                 00d0.1234.4568         7,8,
```

Field description

Field	Description
Ap name	AP Name
Ap-mac	AP MAC Address
radio	Bad Radio ID

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.62 update-key-tsc enable

Use this command to enable the AP device to update key TSC during 802.1x reauthentication. Use the **no** form of this command to disable the AP device to update the key TSC..

update-key-tsc enable

no update-key-tsc enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

AP configuration mode/ AP group configuration mode.

Usage Guide

N/A

Configuration Examples

The following example enables the AP device to update key TSC during 802.1x reauthentication.

```
FS(config)# ap-config AP0001

FS(config-ap)# update-key-tsc enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description	N/A

5 ETH-MNG Commands

5.1 wired-rate

Use this command to configure the maximum bandwidths for various LAN interfaces and slots.

Fit AP: **wired-rate** *value* [**port** *port-id*]

Fat AP: **wired-rate** *value*

Parameter Description

Parameter	Description
value	Specifies the maximum bandwidth in the unit of 1Mbps. The default for AC, AP120-W and AP130-W are 1000, 100 and 1000 respectively.
port-id	Specifies the interface, in the range from 1to 4.There is no default and this parameter is not available on the fat AP.

Defaults

The maximum bandwidths of various LAN interfaces are not limited by default.

Command Modes

Fit AP: AP configuration mode/AP group configuration mode

Fat AP: Interface configuration mode

Usage Guide

If no port is specified, all LAN port bandwidths are configuredd

Configuration Examples

The following example sets the maximum bandwidth for interface0/2of an AP to 50 Mbps.

```
FS(config)#ap-config [ap-name]
FS(config-ap)# wired-rate 50 interface 2
```

The following example sets the maximum bandwidth for interface 0/3for all APs to 30 Mbps.

```
FS(config)#ap-config all
FS(config-ap)# wired-rate 30 interface 3
```

The following example sets the maximum bandwidth for interface0/1 of an AP group to 80 Mbps.

```
FS(config)#ap-group default
FS(config-group)#wired-rate 80 port 1
```

The following example sets the maximum bandwidth for all LAN ports of an AP group to 90 Mbps.

```
FS(config)#ap-group default
FS(config-group)#wired-rate 90
```

Related Commands

Command	Description
show run	Displays the current configuration.

Platform Description

N/A

6 DATA-PLANE Commands

6.1 data-plane

Use this command to configure the forwarding weights of different packets.

Use the **no** form of this command to restore the default setting.

data-plane queue-weight *unicast-packet-weight multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight*

no data-plane queue-weight

Use this command to configure the update interval and token rate of token bucket.

Use the no form of this command to restore the default setting.

data-plane token *token-interval token-base-rate*

no data-plane token

Use this command to enable or disable the wireless broadcast function.

Use the **no** form of this command to restore the default setting.

data-plane wireless-broadcast { **enable** | **disable** }

no data-plane wireless-broadcast

Parameter Description

Parameter	**Description**
queue-weight	Configures the forwarding weights for different packets.
wireless-broadcast	Configures the wireless broadcast function.
unicast-packet-weight	Sets the forwarding weight of unicast packets. The range is from 1 to 100. The default value is 16.
multicast-packet-weight	Sets the forwarding weight of multicast packets. The range is from 1 to 50. The default value is 4.
broadcast-packet-weight	Sets the forwarding weight of broadcast packets. The range is from 1 to 50. The default value is 2.
unknown-multicast-packet-weight	Sets the forwarding weight of unknown multicast packets. The range is from 1 to 25. The default value is 1.
unknown-unicast-packet-weight	Sets the forwarding weight of unknown unicast packets. The range is from 1 to 25. The default value is 1.
token	Configures the update interval and token rate of token bucket.
token-interval	Sets the update interval of the token bucket. The default value is 1 in the unit of 10 milliseconds.
token-base-rate	Sets the token rate of the token bucket. The default value is 64 for AC and 5 for AP.

Defaults The forwarding weight configuration for different types of packets is enabled by default.

The wireless broadcast function is disabled by default.

Command Global configuration mode

Modes

Usage Guide N/A

Configuration Examples The following example configures the forwarding weights of different packet types and enables the wireless broadcast function.

```
FS(config)#data-plane queue-weight 100 50 50 25 25
FS(config)#data-plane token 10 10
FS(config)#data-plane wireless-broadcast enable
```

Platform Description N/A.

7 WLOG Commands

7.1 show wlan diag ap

Use this command to display AP records on an AC.

show wlan diag ap [**ap-mac** *AP_MAC*] [**number** *NUMBER*]

Parameter Description

Parameter	Description
AP_MAC	Specifies the MAC address of an AP to be displayed.
NUMBER	Specifies the maximum number of records to be displayed.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays AP records.

```
FS# show wlan diag ap ap-mac 00d0.f822.33b0 number 10

ap_record: FSAP[00d0.f822.33b0/1.1.1.2],down/up:2

IP Address:1.1.1.2
2012-05-28 09:30:00    [TIMER]          AP UP Time:00:00:18:54
Wired port five in rate/out rate stat:612kbits/sec(in) 1208kbits/sec(out)
    Unicast:      84595     bytes(in) 86625     bytes(out)
    Multicast:    7         bytes(in) 4         bytes(out)
    Broadcast:    2145      bytes(in) 117       bytes(out)
    Error Frame:0           bytes(in) 0         bytes(out)
Radio      channel power       Active STA WEB_Auth    DOT1X       Rssi      ErrorPkt     RetryPkt
-------- ------- ----------- ---------- ---------- ----------    -------- ---------- ----------
1          11        100           2            1           0           0          0           0
2          157       100           0            0           0           0          0           0

IP Address:1.1.1.2
2012-05-28 09:49:18    [CW-DOWN]        AP UP Time:00:00:38:12
Wired port five in rate/out rate stat:187kbits/sec(in) 905kbits/sec(out)
    Unicast:      84789     bytes(in) 86810     bytes(out)
    Multicast:    7         bytes(in) 5         bytes(out)
    Broadcast:    2148      bytes(in) 133       bytes(out)
    Error Frame:0           bytes(in) 0         bytes(out)
Radio      channel power       Active STA WEB_Auth    DOT1X       Rssi      ErrorPkt     RetryCnt
-------- ------- ----------- ---------- ---------- ----------    -------- ---------- ----------
```

```
1      11      100      2       1       0       0       0       0
2      157     100      0       0       0       0       0       0
CAPWAP DOWN REASON:echo expired
```

Field	Description
ap_record	Specifies AP records.
IP Address	Specifies the IP address of an AP whose information is collected.
TIMER	Specifies information collected by a timer.
CW-DOWN	Specifies information collected when a CAPWAP connection is interrupted.
Wired port five in rate/out rate stat	Specifies the input or output rate on a wired port for the recent five minutes.
Unicast	Specifies statistics about unicast packets on a wired port.
Multicast	Specifies statistics about multicast packets on a wired port.
Broadcast	Specifies statistics about broadcast packets on a wired port.
Error Frame	Specifies statistics about incorrect frames on a wired port.
Radio	Specifies a radio ID.
channel	Specifies the working channel of the radio.
power	Specifies the emission frequency of the radio.
Active STA	Specifies the number of STAs associated with the radio.
WEB_AUTH	Specifies the number of STAs associated with the radio and get online through the web interface.
DOT1X	Specifies the number of STAs associated with the radio and get online through 802.1X authentication.
ErrorPkt	Specifies the number of incorrect frames received by the radio.
RetryCnt	Specifies the number of times that packets from the radio are retransmitted.
CAPWAP DOWN REASON	Specifies the reason for CAPWAP disconnection. This item is displayed only when **CW_DOWN** is set.

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on AC devices.

7.2 show wlan diag network

Use this command to display the record information about the entire network.

show wlan diag network

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples

```
FS# show wlan diag network
Time:2012-05-28 09:10:00
AC uptime: 1 h
Online AP:1
Online AP Version:
    PID[AP220-E]:hwver[2.00] AP Number:1
Offline AP:7
ssid                Active STA WEB Auth    Dot1x       Free STA
------------------------------ ---------- ---------- ---------- ----------
1T17-wlog-test1                 0          0          0          0
1T17-wlog-test2                 0          0          0
```

Field	Description
Time	Specifies the time for colleting a record.
AC Running Time	Specifies the running time of an AC connection.
Current Online Number of AP	Specifies the number of online APs.
Online AP Version	Specifies the version of online APs.
Offline Number of AP	Specifies the number of pre-configured but offline APs.
ssid	Specifies the SSID of a WLAN.
Active STA	Specifies the total number of active STAs.
WEB Auth	Specifies the number of STAs that get online through web authentication.
Dot1x	Specifies the number of STAs that get online through 802.1x authentication.
Free STA	Specifies the number of STAs free of authentication.

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on AC devices.

7.3 show wlan diag sta

Use the following command to display STA statistics on an AC:

show wlan diag sta [**sta-mac** *STA_MAC*] [**ip-range** *IP_PREFIX*] [**action** *ACTION* [**result** *RESULT*]] [**number** *NUMBER*]

Use the following command to display STA statistics on an AP:

show wlan diag sta [**sta-mac** *STA_MAC*] [**number** *NUMBER*]

Parameter Description

Parameter	Description
STA_MAC	Specifies the MAC address of an STA.
IP_PREFIX	Specifies the range of IP addresses for the STA, which is limited by an IP prefix.
ACTION	Specifies the type of STA action records.
RESULT	Specifies the result of STA action records.
NUMBER	Specifies the maximum number of records to be displayed.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples This example displays STA statistics on an AC:

```
FS# show wlan diag sta
sta_record: c83a.35c6.0c72
TIME                    IP  Address            Rssi         Link  Rate        AP  MAC                        SSID
RADIO        Action                                  Result     Reason
-------------------      ---------------  -------  -----------  --------------  ----------------------------------  ---------  ------------------------------
------      ------------------------------
09:59:28     192.168.248.2      0            0                  00d0.f822.33b0 lxh-ssid                                          1
STA UP BY APMG                        SUCCESS
10:12:07     192.168.248.2      21           5500               00d0.f822.33b0 lxh-ssid                                          1
STA DOWN BY RSNA                        SUCCESS    AP circular AC user is offline
```

This example displays STA statistics on an AP:

```
FS# show wlan diag sta
sta mac: c83a.35c6.0c72
==========================================================================
=============================================================
2012-05-28 19:31:08
wlan id    state       rssi_rt    rs_rate_mcs tx_frm_cnts rx_frm_cnts tx_frm_flow rx_frm_flow tx_cnts_error
tx_flow_error mgmt_cnts mgmt_flow
-------- -------- -------- ----------- ----------- ----------- ----------- ----------- ------------- ------------- --------- ---------
1             3             23            80                18                59                4384             5967              0
0                     3               381

tx/rxmcs           mcs0, mcs1       mcs2, mcs3       mcs4, mcs5       mcs6, mcs7       mcs8, mcs9       mcs10, mcs11
mcs12, mcs13 mcs14, mcs15
------------- ------------- ------------- ------------- ------------- ------------- ------------- ------------- -------------
txmcspercent : 0             0             0            0            0           0           0         0
rxmcspercent : 0             0             0            0            0           0           0         0

tx/rxrate        1, 2       5.5, 11 6, 9       12, 18    24, 36    48, 54     --           --
------------- ------- ------- ------- ------- ------- ------- ------- -------
txratepercent: 16          0            0            7            50          27          0            0
rxratepercent: 57          3            0            5            13          22          0            0
```

Field	Description
sta_record	Specifies STA records.
TIME	Specifies the time when STA records are collected.
IP Address	Specifies the IP address of an STA whose statistics are collected.
Rssi	Specifies signal strength.
Link Rate	Specifies a connection rate.
AP MAC	Specifies the MAC address of an AP associated with the STA.
SSID	Specifies the SSID of the WLAN associated with the STA.
RADIO	Specifies the ID of the radio associated with the STA.
Action	Specifies the type of STA action records.
Result	Specifies the result of STA action records.
Reason	Specifies the reason for STA action records.

Related Commands

Command	Description
N/A	N/A

Platform This command is supported on ACs.

Description

7.4 wlan diag enable

Use this command to enable the WLAN log (WLOG) . Use the **no** form of this command to disable WLOG.

wlan diag enable

no wlan diag enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults The WLOG function is disabled on ACs and APs.

Command Mode Global configuration mode

Usage Guide The memory pre-allocation is performed when the WLAN-WLOG function is enabled. If the memory is insufficient, the WLAN-WLOG function cannot be enabled.

Memories of all saved information and pre-allocated memories are set free when the WLOG function is disabled.

Configuration Examples The following example enables and disables the WLOG function:

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#wlan diag enable
FS(config)#no wlan diag enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on ACs.

7.5 web-server enable api-path assoc-sta url

Use this command to configure the Elog server URL for the associated STA. Use the **no** form of this command to remove the setting.

web-server enable api-path assoc-sta url *url*

Use this command to delete Elog server URLs.

no web-server enable api-path assoc-sta url

Parameter

Parameter	Description

Description

url	Sets the Elog server URL

Defaults

No Elog server is configured by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures an Elog server URL and removes the settings.

```
FS# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
FS(config)#web-server enable api-path assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta
FS(config)#no web-server enable api-path assoc-sta url
http://172.18.155.14:8080/elog/service/dc/updateSta
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on ACs.

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.