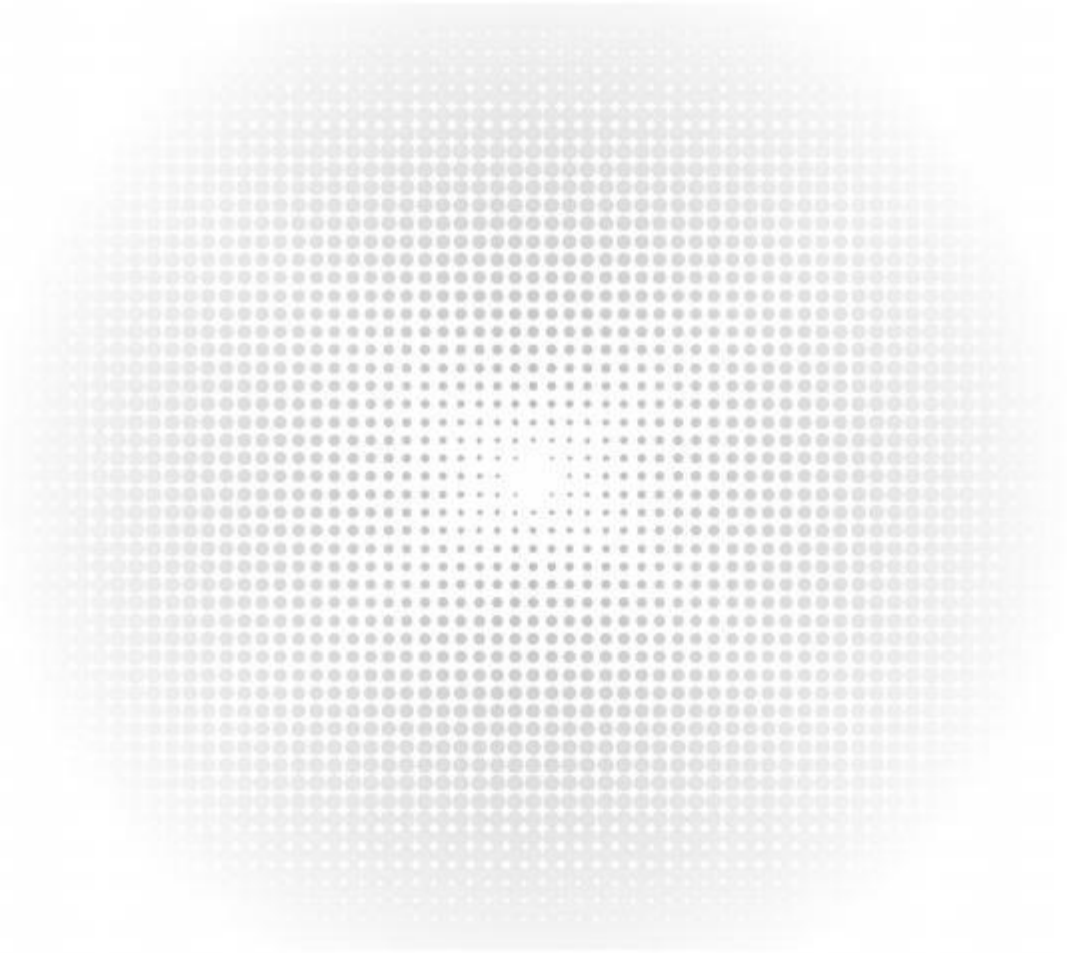
N Series Switches

Configuration Guide

Models: N8550-48B8C; N8550-32C



CONFIGURATION GUIDE

Contents

List of Figures

1 Basic Configuration Guide

1.1 User Management Configuration

1.1.1 Overview

Function Introduction

Only one user can enter configuration mode at a time.

User management increases the security of the system by keeping the unauthorized users from guessing the password. The user is limited to a specific number of attempts to successfully log in to the switch.

There are three load modes in the switch.

- In “no login” mode, anyone can load the switch without authentication.
- In “login” mode, there is only one default user.
- In “login local” mode, if you want to load the switch you need to have a user account. Local user authentication uses local user accounts and passwords that you create to validate the login attempts of local users. Each switch has a maximum of 32 local user accounts. Before you can enable local user authentication, you must define at least one local user account. You can set up local user accounts by creating a unique username and password combination for each local user. Each username must be fewer than 32 characters. You can configure each local user account with a privilege level; the valid privilege levels are 1 or 4. Once a local user is logged in, only the commands those are available for that privilege level can be displayed.

There is only one user can enter the configure mode at the same time.

Principle Description

N/A

1.1.2 Configuration

Configuring user levels

step 1 Enter the configuration mode

```
switch# configure
```

step 2 Create the username and password

```
Switch(config)# username admin password 12345
```

step 3 Enter the user management mode and set authentication mode,then exit

```
Switch(config)# exit
Switch(config)# line vty 1 7
Switch(config-line)# enable password level 3 cipher 12345
Switch(config-line)# login authentication local
```

```
Switch(config-line)# exit
```

step 4 Exit configuration mode

```
Switch(config)# exit
```

step 5 Validation

After above configuration,the system will first prompt the user to enter the user name when logging in the switch:

```
Username:
```

After you enter your user name, you are prompted for a password:

```
Username: admin
Password: *****
```

User Management Configuration

step 1 Enter the configure mode

```
switch# configure
```

step 2 enter user management mode and set authentication mode and login password,then exit

```
Switch(config)# line vty 0 7
Switch(config-line)# login
Switch(config-line)# enable password cipher 12345
```

step 3 Exit the configure mode

```
switch(config)# exit
```

step 4 Validation

After the above configuration, the system will prompt the following authentication information when logging in the switch, and the user can log in with the password previously created.

```
Password:*****
```

Configuring Password recovery procedure

step 1 connect the switch through console line and power it up,the console display as follows,select ONIE

```
                                GNU GRUB  version 2.02

 +----------------------------------------------------------------------------+
```

```
|FSOS                                                                    |
|*ONIE                                                                   |
|                                                                        |
|                                                                        |
|                                                                        |
|                                                                        |
|                                                                        |
|                                                                        |
|                                                                        |
|                                                                        |
|                                                                        |
|                                                                        |
+------------------------------------------------------------------------+

      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands
      before booting or `c' for a command-line.
```

Step 2 Enter ONIE selection interface and enter ONIE:Embed ONIE node

```
                                GNU GRUB  version 2.02

+------------------------------------------------------------------------+
| ONIE: Install OS                                                       |
| ONIE:Rescue                                                            |
| ONIE: Uninstall OS                                                     |
| ONIE: Update ONIE                                                      |
|*ONIE: Embed ONIE                                                       |
| DIAG: Accton Diagnostic (accton_as7326_56x)                            |
|                                                                        |
|
|                                                                        |
|
|                                                                        |
|
+------------------------------------------------------------------------+
```

Step 3:make the switch restore default username and password

```
ONIE:/ # sed -i 's/username admin group administrators password .*./username adm
in group administrators password $1$kijv$bIP5gEaeX6wG6eQLeT3Di0/g' /mnt/onie-boo
t/mtd/startcfg
ONIE:/ # reboot
```

Note ： Please remember your username and password.Recovering the password may lead configuration lost or service interrupted; we strongly recommend that user should remember the username and password.

1.1.3 Application cases

N/A

1.2 Configuring TFTP

1.2.1 Overview

Function Introduction

Trivial File Transfer Protocol (TFTP) is a simple File Transfer Protocol used in the TCP/IP Protocol family for simple File Transfer between client and server, providing a File Transfer service with little complexity and overhead.The port number is 69.This protocol is designed for small file transfers.So it doesn't have many of the usual features of FTP, it can only get or write files from the file server, it can't list directories, it doesn't authenticate, it transfers 8-bit data.

Principle Description

N/A

1.2.2 Configuration

Before uploading and downloading, you need to do the following:

Make sure your workstation is configured correctly as a TFTP server.

Make sure the Switch to TFTP server route is accessible.If there is no router for routing communication between subnets, the switch and the TFTP server must be on the same network.The ping command checks whether you can connect to the TFTP server.

Make sure that the configuration files to be downloaded are in the correct directory on the TFTP server.

Download to make sure the permissions on the file are set correctly.

The upload operation, if you want to overwrite an existing file (including an empty file) on the server, ensures that the permissions for that file are set correctly.

Downloading a configuration file by using TFTP in IPv4 network

```
switch# configure
switch(config)# tftp get 172.100.10.190 onie-installer
```

Uploading a configuration file by using TFTP in IPv4 network

```
switch# configure
switch(config)# tftp put 172.100.10.190 config.txt config
```

Downloading a configuration file by using TFTP in IPv6 network

```
#Switch# configure
Switch(config)# tftp get 2012::1 onie-installer
```

Uploading a configuration file by using TFTP in IPv6 network

```
Switch# configure
Switch(config)# tftp put 2012::1 config.txt config
```

1.2.3 Application cases

N/A

1.3 Configuring telnet

1.3.1 Overview

Function Introduction

Telnet protocol is a member of TCP/IP protocol family, and it is the standard protocol and main method of Internet remote login service.It provides the user with the ability to perform work on the remote login host on the local computer.Use the Telnet program on the end user's computer to connect to the server.The end user can enter commands in the Telnet program, and these commands run on the server as if they were entered directly on the server console.With the Telnet program, the user can control the server locally.To start a Telnet session, you must enter a user name and password to log in to the server.Telnet is a commonly used method of remotely controlling a Web server.

Principle Description

N/A

1.3.2 Configuration

Configuring Telnet to other switches with an inner port

Example 1:ipv4

```
Switch# telnet 10.1.12.2
  Press 'Ctrl+\' to quit.
User Access Verification
Username: admin
Password: *****
Switch#
```

Example 1:ipv6

```
Switch# telnet6 2012::2
  Press 'Ctrl+\' to quit.
User Access Verification
Username: admin
Password: *****
Switch#
```

Configuring Telnet to other switches through management port

Example 1:ipv4

```
Switch# telnet 10.32.133.119
 Press 'Ctrl+\' to quit.
User Access Verification
Username: admin
Password: *****
Switch#
```

Example 1:ipv6

```
Switch# telnet6 2001::2
 Press 'Ctrl+\' to quit.
User Access Verification
Username: admin
Password: *****
Switch#
```

Configuring the Telnet service for the switch

step 1 Enter the configuration mode

```
switch# configure
```

step 2 Enabling Telnet server

```
Switch(config)# telnetd
```

step 3 Exit configuration mode

```
switch(config)# exit
```

1.3.3 Application cases

N/A

1.4 Saving the Configuration File

1.4.1 Overview

Function Introduction

You can run commands to modify the current configuration of the device, but the modified configuration will be lost after the device restarts. To enable the new configuration to still take effect after a restart, save the current configuration in the configuration file before restarting the device.

Principle Description

N/A

1.4.2 Configuration

Save configuration manually

switch# write file

This will save the configuration in the flash memory.

Are you sure?(y/n) [y] y
Building configuration,please wait for a moment.....

[OK]

1.4.3 Application cases

N/A

1.5 Clearing the Configuration File

1.5.1 Overview

Function Introduction

After the device software is upgraded, the configuration file in the storage device may not match the new version of the software. In this case, this command can be used to clear the old startup configuration file.If the used device is applied to the new environment, the original configuration file cannot meet the requirements of the new application, and the device needs to be reconfigured, then this command can be used to clear the old startup configuration file.After using this command, if you do not re-save the configuration file using the writefile command, the next time the device starts, the default configuration parameters will be used for system initialization.

Principle Description

N/A

1.5.2 Configuration

Clear the boot profile of the system on the storage device

switch(config)#erase startup-config

This will erase the configuration in the flash memory.

Are you sure?(y/n) [y] y

1.5.3 Application cases

N/A

1.6 Restarting the Device

1.6.1 Overview

Function Introduction

This command functions as a cold boot.Using this command, the remote maintenance of the device does not require the user to go to the device location to restart, but can restart the device directly from a remote location.In general, this command is not allowed, as it will cause the network to work down for a short time.In addition, when restarting the device, it is recommended that the user first confirm whether the configuration file needs to be saved.

Principle Description

N/A

1.6.2 Configuration

Restart the device

```
Switch# configure
switch(config)#reboot
                WARNING:System will reboot! Continue?(y/n) [y] y
System nowis rebooting,please wait.
```

1.6.3 Application cases

N/A

2 Ethernet Configuration Guide

2.1 Configuring Interface

2.1.1 Overview

Function Introduction

Interface status, When the interface is configured as "no shutdown", it can work normally after cable is connected. When the interface is configured as "shutdown", no matter the cable is connected or not, the interface can not work. Ethernet interfaces for switches can be divided into two categories depending on the business functions hosted by the interfaces：

- Mgt-eth:the Management interface mainly provides configuration management support for users, that is, users can log in to the device and perform configuration and management operations through such an interface.The management interface does not undertake the business transport.
- Business interface: It is mainly responsible for receiving and sending business data

According to the rate supported by the interface, the Ethernet interface of the switch can be divided into:

- 10gigaethernet
- 25 gigaethernet
- 40 gigaethernet
- 100 gigaethernet

Principle Description

N/A

2.1.2 Configuration

Configuring Interface State

step 1 Enter the configure mode

```
switch# configure
```

step 2 Turn on an interface

```
swtch#(config)# interface 10g1/0/1
switch(config-10ge1/0/1)#no shutdown
```

step 3 Shut down an interface

```
swtch#(config)# interface 10g1/0/2
switch(config-10ge1/0/1)#shutdown
```

step 4 Exit the configure mode

```
Switch(config-10ge1/0/1)# end
```

step 5 Validation

Use the following command to display the status of the interfaces:

```
switch(config)#show interface
  Interface              State(a/o)   Mode          Descr
  mgt-eth0/0/0           up/up        router        -
  10ge1/0/1              up/down      bridge        -
  10ge1/0/2              down/down    bridge        -
```

Configuring Interface Speed

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode and set the speed

Set speed of interface 100gigaethernet 1/0/1 to 40000M (Only 100G port supports this command)

```
switch(config)#interface 100gigaethernet 1/0/1
switch(config-100ge1/0/1)#speed 1\40000
switch(config-100ge1/0/1)#no shutdown
```

step 3 Exit the configure mode

```
switch(config-100ge1/0/1)# end
```

step 4 Validation

Use the following command to display the status of the interfaces:

```
Interface 100gigaethernet1/0/1 admin state : up
 Line protocol current state : down
 The reason for down is link-down
 Switch Port, PVID : 1, The Maximum Frame Length is 9216
 IP Sending Frames' Format is PKTFMT_ETHNT_2,Hardware address is 68:21:5f:fb:08:54
 Current system time: 2000-01-01 17:26:51
 Port Mode: optical
 Speed : 40000(Mbps),       Duplex: full,    Negotiation: disable
 Last 300 seconds input rate: 0 Bps, 0 pps, 0 bps
 Last 300 seconds output rate: 0 Bps, 0 pps, 0 bps
 Input peak rate 0/0 Bps, Record time: ----
 Output peak rate 0/0 Bps, Record time: ----
```

```
Input:  0/0 packets,  0/0 bytes
  Unicast          :          0/0          , Multicast          :          0/0
  Broadcast        :          0/0          , Jumbo              :          0/0
  CRC              :          0/0          , Giants             :          0/0
  Jabbers          :          0/0          , Fragments          :          0/0
  Runts            :          0/0          , DropEvents         :          0/0
  Alignments       :          0/0          , Symbols            :          0/0
  Ignoreds         :          0/0          , Frames             :          0/0
  Discard          :          0/0          , Total Error        :          0/0
Output:  0/0 packets,  0/0 bytes
  Unicast          :          0/0          , Multicast          :          0/0
  Broadcast        :          0/0          , Jumbo              :          0/0
  Collisions       :          0/0          , Deferreds          :          0/0
  Late Collisions  :          0/0          ,Excessive Collisions:          0/0
  Buffers Purged   :          0/0          , Discard            :          0/0
  Total Error      :          0/0
Input bandwidth utilization : 0.00%
Output bandwidth utilization : 0.00%
```

Configuring Interface Duplex

The port duplex mode defaults to full duplex. When the port is can receive packets while sending them, the port is set to the full property.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode and set the duplex

Set duplex of interface 10g1/0/33 to full

```
switch(config)#interface 10gigaethernet 1/0/33
switch(config-10ge1/0/33)#no shutdown
switch(config-10ge1/0/33)#duplex full
```

step 3 Validation

Use the following command to display the status of the interfaces:

```
Interface 10gigaethernet1/0/33 admin state : up
Line protocol current state : down
The reason for down is link-down
Switch Port, PVID : 1, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2,Hardware address is 68:21:5f:fb:08:54
Current system time: 2000-01-01 17:31:54
Port Mode: optical
Speed : 10000(Mbps),      Duplex: full,    Negotiation: disable
```

```
Last 300 seconds input rate: 0 Bps, 0 pps, 0 bps
Last 300 seconds output rate: 0 Bps, 0 pps, 0 bps
Input peak rate 0/0 Bps, Record time: ----
Output peak rate 0/0 Bps, Record time: ----
Input:  0/0 packets,  0/0 bytes
  Unicast          :        0/0          , Multicast          :        0/0
  Broadcast        :        0/0          , Jumbo              :        0/0
  CRC              :        0/0          , Giants             :        0/0
  Jabbers          :        0/0          , Fragments          :        0/0
  Runts            :        0/0          , DropEvents         :        0/0
  Alignments       :        0/0          , Symbols            :        0/0
  Ignoreds         :        0/0          , Frames             :        0/0
  Discard          :        0/0          , Total Error        :        0/0
Output:  0/0 packets,  0/0 bytes
  Unicast          :        0/0          , Multicast          :        0/0
  Broadcast        :        0/0          , Jumbo              :        0/0
  Collisions       :        0/0          , Deferreds          :        0/0
  Late Collisions  :        0/0          , Excessive Collisions:       0/0
  Buffers Purged   :        0/0          , Discard            :        0/0
  Total Error      :        0/0
Input bandwidth utilization : 0.00%
Output bandwidth utilization : 0.00%
```

2.1.3 Application cases

N/A

2.2 Configuring Layer3 Interfaces

2.2.1 Overview

Function Introduction

- VLAN interfaces: Logical interface with layer3 features. Connect different VLANs via IP address on the VLAN interface. VLAN interfaces can be created and deleted.

A Layer 3 switch can have an IP address assigned to each routed port and VLAN interface. All Layer 3 interfaces require an IP address to route traffic. This section shows how to configure an interface as a Layer 3 interface and how to assign an IP address to an interface.

Principle Description

N/A

2.2.2 Configuration

Configuring vlanif Interfaces

This chapter describes configuring VLAN interfaces and using them. Several Virtual LAN (VLAN) interfaces can be configured on a single Ethernet interface. Once created, a VLAN interface functions the same as any physical interface, and it can be configured

and displayed like any physical interface. Routing protocols, such as, RIP, OSPF and BGP can run across networks using VLAN interfaces.

step 1 Enter the configure mode

```
switch# configure
```

step 2 create a vlan

```
switch(config)#vlan 10
switch(vlan-10)#exit
```

step 3 Enter the interface configure mode and set switch port attributes

```
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#port link-type trunk
switch(config-10ge1/0/1)#port trunk allow-pass vlan 10
switch(config-10ge1/0/1)#no shutdown
switch(config-10ge1/0/1)#exit
```

step 4 Enter the vlan interface configure mode and set IP address

```
switch(config)#interface vlan 10
switch(config-vlanif-10)#ip address 2.2.2.2/24
```

step 5 Exit the configure mode

```
switch(config-vlanif-10)#end
```

step 6 Validation

Use the following command to display the brief status of the interfaces:

```
switch(config)#show ip interface
 The total number of ip address: 3
  Ip-Address          Interface          IPIndex State(a/o)Role      Type       Vpn-instance
  2.2.2.2/24          vlan10             1       up/down   primary   static     N/A
```

2.2.3 Application cases

N/A

2.3 Configuring MAC Address Table

2.3.1 Overview

Function Introduction

MAC address table contains address information for the switch to forward traffic between ports. The address table includes these types of address:

- Dynamic address: the source address learnt by the switch and will be aged after aging time if this address is not hit. We only support IVL learning mode.
- Static address: the source address manually added by administrators.

Following is a brief description of terms and concepts used to describe the MAC address table:

- IVL: Independent VLAN Learning: for a given set of VLANs, if a given individual MAC Address is learned in one VLAN, it can't be used in forwarding decisions taken for that address relative to any other VLAN in the given set.
- SVL: Shared VLAN Learning: for a given set of VLANs, if an individual MAC Address is learned in one VLAN, it can be used in forwarding decisions taken for that address relative to all other VLANs in the given set.

Reference to standard:IEEE 802.1D，IEEE 802.1Q

Principle Description

N/A

2.3.2 Configuration

Configuring Address Aging Time

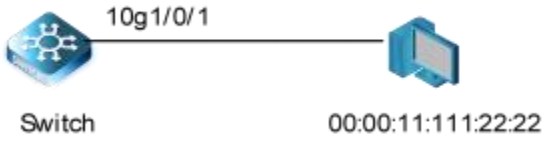


Figure 2-1 Mac address aging

The aging time is not exact time. If aging time set to N, then the dynamic address will be aged after N~2N interval. The default aging time is 300 seconds.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Set dynamic address aging time

```
switch(config)#mac aging-time 200
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

Use the following command to display the aging time:

```
switch#show mac info
Aging time:200 seconds
```

Configuring Static Unicast Address

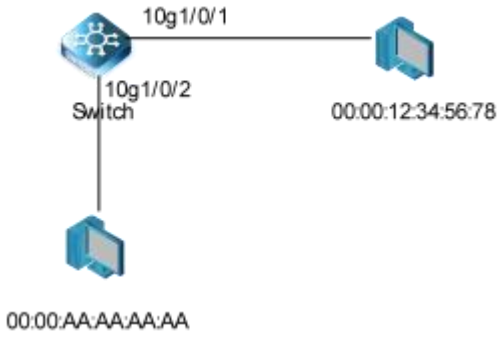


Figure 2-2 Static mac address table

Unicast address can be only bound to one port. According to the picture, Mac-Da 00:00:12:34:56:78 should forward via 10g1/0/1.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Set static mac address table

```
switch(config)#mac-address static 10 00:00:12:34:56:78 10gigaethernet 1/0/1
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

Use the following command to display the mac address table:

```
switch(config)#show mac-address

  Total              :1
  Static             :1
  Dynamic            :0
```

```
Blackhole          :0
Sticky             :0
Security           :0
Snooping           :0
Valid              :1

MAC Address              Vlan/Vsi/BD Interface       Oper-Type          Type
00:00:12:34:56:78   10/--/--     10ge1/0/1      forward            static
```

Configuring MAC Filter Address

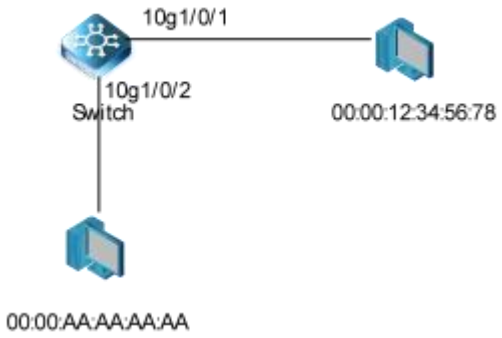


Figure 2-3 mac address filter

MAC filter will discard these frames whose source or destination address is set to discard. The MAC filter has higher priority than MAC address.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Add unicast address to be discarded

```
switch(config)#mac-address blackhole 10 00:00:12:34:56:78
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

Use the following command to display the mac address filter:

```
switch#show show mac-address blackhole

  Blackhole          :1

  MAC Address              Vlan/Vsi/BD   Interface       Oper-Type          Type
  00:00:12:34:56:78         10/--/--      N/A             discard            black-hole
```

2.3.3 Application cases

N/A

2.4 Configuring VLAN

2.4.1 Overview

Function Introduction

VLAN (Virtual Local Area Network) is a switched network that is logically segmented the network into different broadcast domain so that packets are only switched between ports that are designated for the same VLAN. Each VLAN is considered as a logical network, and packets send to stations that do not belong to the same VLAN must be forwarded through a router.

Reference to standard: IEEE 802.1Q

Principle Description

Following is a brief description of terms and concepts used to describe the VLAN:

- VID: VLAN identifier
- LAN: Local Area Network
- VLAN: Virtual LAN
- PVID: Port VID, the untagged or priority-tagged frames will be assigned with this VID

Tagged Frame: Tagged Frame is inserted with 4 Bytes VLAN Tag, show in the picture below:

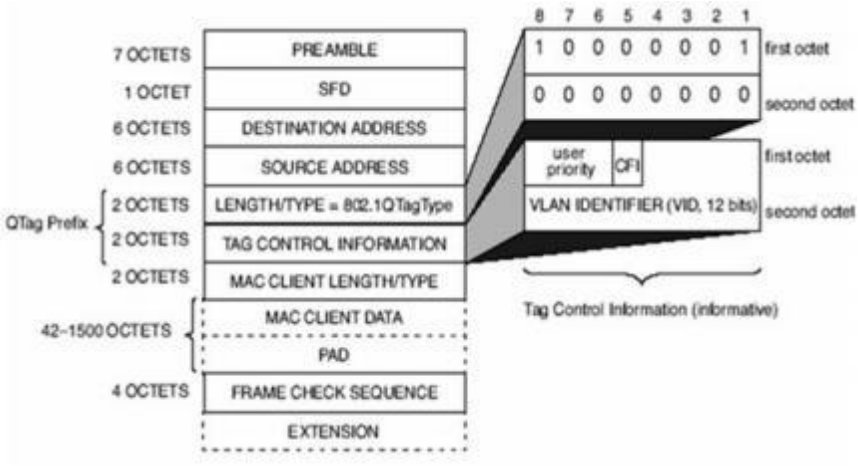


Table 1 Frame processing based on the port type

Port Type	Untagged Frame Processing	Tagged Frame Processing	Frame Transmission
Access	Accepts an untagged frame	Accepts the tagged frame if the frame's VLAN ID matches the	After the PVID tag is stripped, the frame is

port		default VLAN ID.	transmitted.
		Discards the tagged frame if the frame's VLAN ID differs from the default VLAN ID.	
Trunk port	When the default VLAN ID is in the allowed VLAN ID list, the message is received.	Accepts a tagged frame if the VLAN ID carried in the frame is permitted by the port	If the frame's VLAN ID matches the default VLAN ID and the VLAN ID is permitted by the port, the switch removes the tag and transmits the frame.
	When the default VLAN ID is not in the allowed VLAN ID list, the message is discarded.	Discards a tagged frame if the VLAN ID carried in the frame is denied by the port.	If the frame's VLAN ID differs from the default VLAN ID, but the VLAN ID is still permitted by the port, the switch will directly transmit the frame.
Hybrid port	When the default VLAN ID is in the allowed VLAN ID list, the message is received. (default PVID allowed)	Accepts a tagged frame if the VLAN ID carried in the frame is permitted by the port.	When the VLAN ID is the VLAN ID of the untag allowed by the interface, split the original tag and send the message.
	When the default VLAN ID is not in the allowed VLAN ID list, the message is discarded.	Discards a tagged frame if the VLAN ID carried in the frame is denied by the port.	When the VLAN ID is the VLAN ID with tag allowed by the interface, keep the original tag to send the message.

Figure 2-4 Trunk link

Trunk Link: Both tagged and untagged frames can be transmitted on this link. Trunk link allow for multiple VLANs to cross this link, show in the picture below:

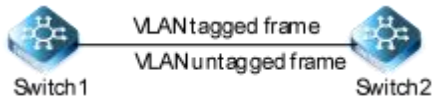
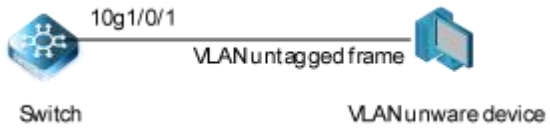


Figure 2-5 Access link

Access Link: connects a host to a switch. Generally, a host does not know which VLAN it belongs to, and host hardware cannot distinguish frames with VLAN tags. Therefore, hosts send and receive only untagged frames. show in the picture below:



2.4.2 Configuration

Configuring Access Port

Figure 2-7 Access link

an access port on a switch connects to the port on a host. The access port can only connect to an access link. Only the VLAN whose ID is the same as the default VLAN ID is allowed on the access port. Ethernet frames sent from the access port are untagged frames.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the vlan configure mode and create vlan

```
switch(config)# vlan 2
switch(vlan-2)#exit
```

step 3 Enter the interface configure mode, set the switch port mode and bind to the vlan

```
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#port link-type access
switch(config-10ge1/0/1)#port default vlan 2
```

step 4 Exit the configure mode

```
switch(config-10ge1/0/1)# end
```

step 5 Validation

Use the following command to display the information of the switch port interface:

```
switch(config-10ge1/0/1)#show
!
interface 10gigaethernet 1/0/1
 port link-type access
 port default vlan 2
```

Use the following command to display the vlan brief information:

```
switch(config)#show vlan verbose
```

VLAN ID:1

Vlan alias:N/A
The total number of ipv4 address is:0,ipv6 address is:0
Unknown-multicast:forward
Unknown-unicast:forward
Admin status:up
Physical status:up
Vlan-status:static
Member(s):

Interface	Tagged
40ge1/0/54	Untag
40ge1/0/53	Untag
40ge1/0/52	Untag
40ge1/0/51	Untag
40ge1/0/50	Untag
40ge1/0/49	Untag
10ge1/0/48	Untag
10ge1/0/47	Untag
10ge1/0/46	Untag
10ge1/0/45	Untag
10ge1/0/44	Untag
10ge1/0/43	Untag
10ge1/0/42	Untag
10ge1/0/41	Untag
10ge1/0/40	Untag
10ge1/0/39	Untag
10ge1/0/38	Untag
10ge1/0/37	Untag
10ge1/0/36	Untag
10ge1/0/35	Untag
10ge1/0/34	Untag
10ge1/0/33	Untag
10ge1/0/32	Untag
10ge1/0/31	Untag
10ge1/0/30	Untag
10ge1/0/29	Untag
10ge1/0/28	Untag
10ge1/0/27	Untag
10ge1/0/26	Untag
10ge1/0/25	Untag
10ge1/0/24	Untag
10ge1/0/23	Untag
10ge1/0/22	Untag
10ge1/0/21	Untag
10ge1/0/20	Untag
10ge1/0/19	Untag
10ge1/0/18	Untag
10ge1/0/17	Untag

```
        10ge1/0/16                    Untag
        10ge1/0/15                    Untag
        10ge1/0/14                    Untag
        10ge1/0/13                    Untag
        10ge1/0/12                    Untag
        10ge1/0/11                    Untag
        10ge1/0/10                    Untag
        10ge1/0/9                     Untag
        10ge1/0/8                     Untag
        10ge1/0/7                     Untag
        10ge1/0/6                     Untag
        10ge1/0/5                     Untag
        10ge1/0/4                     Untag
        10ge1/0/3                     Untag
        10ge1/0/2                     Untag
VLAN ID:2
        Vlan alias:N/A
        The total number of ipv4 address is:0,ipv6 address is:0
        Unknown-multicast:forward
        Unknown-unicast:forward
        Admin status:up
        Physical status:down
        Vlan-status:static
        Member(s):
          Interface                   Tagged
          10ge1/0/1                   Untag
```

Configuring Trunk Port

Trunk port receives tagged, untagged, and priority-tagged frames, and transmits both untagged and tagged frames. If trunk port receives an untagged frame, this frame will be assigned to the VLAN of the trunk port's PVID; if a frame send out from the trunk port and the frame's VID is equal to the trunk port's PVID, this frame will be send out without VLAN tag.

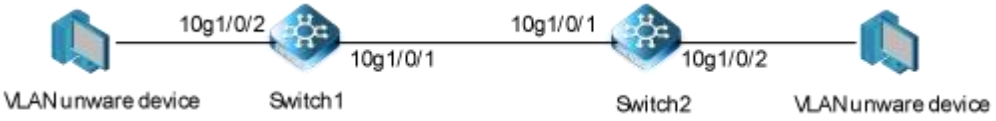


Figure 2-8 Trunk link

Network topology is shown in the picture above. The following configuration steps are same for Switch1 and Switch2.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the vlan configure mode and create vlan

```
switch(config)#vlan 10 20
Switch(config)# exit
```

step 3 Enter the interface configure mode, set the switch port mode and bind to the vlan

Set 10g1/0/1's switch port mode as trunk, set native vlan as 10, and allow all VLANs on this interface:

```
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#port link-type trunk
switch(config-10ge1/0/1)#port trunk allow-pass vlan all
switch(config-10ge1/0/1)#port trunk pvid 10
switch(config-10ge1/0/1)#exit
```

Set 10g1/0/2's switch port mode as access, and bind to vlan 10:

```
switch(config)#interface 10gigaethernet 1/0/2
switch(config-10ge1/0/2)#port link-type access
switch(config-10ge1/0/2)#port default vlan 10
switch(config-10ge1/0/2)#exit
```

step 4 Exit the configure mode

```
switch(config-10ge1/0/2)#end
```

step 5 Validation

Use the following command to display the information of the switch port interface:

```
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#show
!
interface 10gigaethernet 1/0/1
 port link-type trunk
 port trunk allow-pass vlan all
 port trunk pvid 10
switch(config-10ge1/0/1)#q
switch(config)#interface 10gigaethernet 1/0/2
switch(config-10ge1/0/2)#show
!
interface 10gigaethernet 1/0/2
 port link-type access
 port default vlan 10
```

Use the following command to display the vlan brief information:

```
switch(config)#show vlan verbose
VLAN ID:1
```

Vlan alias:N/A
The total number of ipv4 address is:0,ipv6 address is:0
Unknown-multicast:forward
Unknown-unicast:forward
Admin status:up
Physical status:up
Vlan-status:static
Member(s):

Interface	Tagged
10ge1/0/1	Tag
40ge1/0/54	Untag
40ge1/0/53	Untag
40ge1/0/52	Untag
40ge1/0/51	Untag
40ge1/0/50	Untag
40ge1/0/49	Untag
10ge1/0/48	Untag
10ge1/0/47	Untag
10ge1/0/46	Untag
10ge1/0/45	Untag
10ge1/0/44	Untag
10ge1/0/43	Untag
10ge1/0/42	Untag
10ge1/0/41	Untag
10ge1/0/40	Untag
10ge1/0/39	Untag
10ge1/0/38	Untag
10ge1/0/37	Untag
10ge1/0/36	Untag
10ge1/0/35	Untag
10ge1/0/34	Untag
10ge1/0/33	Untag
10ge1/0/32	Untag
10ge1/0/31	Untag
10ge1/0/30	Untag
10ge1/0/29	Untag
10ge1/0/28	Untag
10ge1/0/27	Untag
10ge1/0/26	Untag
10ge1/0/25	Untag
10ge1/0/24	Untag
10ge1/0/23	Untag
10ge1/0/22	Untag
10ge1/0/21	Untag
10ge1/0/20	Untag
10ge1/0/19	Untag
10ge1/0/18	Untag
10ge1/0/17	Untag

```
        10ge1/0/16                    Untag
        10ge1/0/15                    Untag
        10ge1/0/14                    Untag
        10ge1/0/13                    Untag
        10ge1/0/12                    Untag
        10ge1/0/11                    Untag
        10ge1/0/10                    Untag
        10ge1/0/9                     Untag
        10ge1/0/8                     Untag
        10ge1/0/7                     Untag
        10ge1/0/6                     Untag
        10ge1/0/5                     Untag
        10ge1/0/4                     Untag
        10ge1/0/3                     Untag
VLAN ID:10
        Vlan alias:N/A
        The total number of ipv4 address is:0,ipv6 address is:0
        Unknown-multicast:forward
        Unknown-unicast:forward
        Admin status:up
        Physical status:down
        Vlan-status:static
        Member(s):
          Interface                   Tagged
          10ge1/0/2                     Untag
          10ge1/0/1                     Untag
VLAN ID:20
        Vlan alias:N/A
        The total number of ipv4 address is:0,ipv6 address is:0
        Unknown-multicast:forward
        Unknown-unicast:forward
        Admin status:up
        Physical status:down
        Vlan-status:static
        Member(s):
          Interface                   Tagged
          10ge1/0/1                     Tag
```

2.4.3 Application cases

N/A

2.5 Configuring QinQ

2.5.1 Overview

Function Introduction

Ethernet is widely used on ISP networks, but 802.1Q VLANs are unable to identify and isolate large numbers of users on metro Ethernet networks because the 12-bit VLAN tag field defined in IEEE 802.1Q only identifies a maximum of 4096 VLANs. QinQ was developed to expand VLAN space beyond 4096 VLANs so that a larger number of users can be identified on a metro Ethernet network.

QinQ was originally developed to expand VLAN space by adding an additional 802.1Q tag to an 802.1Q-tagged packet. In this way, the number of VLANs can increase to 4094 x 4094 (values 0 and 4095 are reserved). Packets are forwarded based on outer VLAN tags on the public network, and devices on the public network add outer VLAN IDs to MAC address tables of the corresponding VLANs. Inner VLAN tags of packets are transmitted as data on the public network.

Principle Description

N/A

2.5.2 Configuration

Configuring 802.1q Tunneling （Basic QinQ）

Figure 2-11 QinQ Tunnel

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode, set the switch port mode

```
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#port link-type dot1q-tunnel
switch(config-10ge1/0/10)#port default vlan 20
```

step 3 Exit the configure mode

```
switch(config-10ge1/0/1)#end
```

step 4 Validation

This example shows how to configure a switchport to basic dot1q-tunnel port. You can use show the configuration on the switchport

```
interface 10gigaethernet 1/0/1
 port link-type dot1q-tunnel
```

Configuring 802.1q Tunneling （Selective QinQ.）

Figure 2-12 QinQ Tunnel

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the vlan configure mode and create vlan

```
switch(config)#vlan 30-40,200,300
switch(config)#exit
```

step 3 enable qinq under the interface

```
switch(config-10ge1/0/1)#vlan-stacking enable
```

step 4 QinQ function is flexible to configure single VLAN and batch VLAN.

```
switch(config-10ge1/0/1)#vlan-mapping vlan 20 map-vlan 200
switch(config-10ge1/0/1)#vlan-mapping vlan 30 to 40 map-vlan 300
```

step 5 Configure port properties.

10ge1/0/1:

```
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#port link-type hybrid
switch(config-10ge1/0/1)#port hybrid vlan 200,300 untagged
```

10ge1/0/2:

```
switch(config)#interface 10gigaethernet 1/0/2
switch(config-10ge1/0/2)#port link-type trunk
switch(config-10ge1/0/2)#port trunk allow-pass vlan 200,300
```

step 6 Exit the configure mode

```
switch(config-10ge1/0/2)# end
```

step 7 Validation

This example shows how to configure a switchport to selective dot1q-tunnel port:

```
switch(config-10ge1/0/1)#show
                                                                                !
interface 10gigaethernet 1/0/1
 port hybrid vlan 200,300 untagged
 vlan-stacking enable
 vlan-stacking vlan 20 stack-vlan 200
 vlan-stacking vlan 30 to 40 stack-vlan 300

switch(config)#interface 10gigaethernet 1/0/2
switch(config-10ge1/0/2)#show
                                                                                !
interface 10gigaethernet 1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200,300
```

Use the following command to display the information of the vlan mapping table：

```
switch(config)#show vlan-mapping config
 interface 10gigaethernet 1/0/1
 interface 100ge1/0/1

 vlan-stacking enable
 vlan-stacking vlan 20 stack-vlan 200
 vlan-stacking vlan 30 to 40 stack-vlan 300
```

2.6 Configuring VLAN Mapping

2.6.1 Overview

Function Introduction

In some scenarios, two Layer 2 user networks in the same VLAN are connected through the backbone network. To implement Layer 2 connectivity between users and deploy Layer 2 protocols such as MSTP uniformly, the two user networks need to seamlessly interwork with each other. In this case, the backbone network needs to transmit VLAN packets from the user networks. Generally, VLAN plan on the backbone network and user network is different, so the backbone network cannot directly transmit VLAN packets from a user network.

One method is to configure a Layer 2 tunneling technology such as QinQ or VPLS to encapsulate VLAN packets into packets on the backbone network so that VLAN packets are transparently transmitted. However, this method increases extra cost because packets are encapsulated. In addition, Layer 2 tunneling technology may not support transparent transmission of packets of some protocol packets. The other method is to configure VLAN mapping. When VLAN packets from a user network enter the backbone network, an edge device on the backbone network changes the C-VLAN ID to the S-VLAN ID. After the packets are transmitted to the other side, the edge device changes the S-VLAN ID to the C-VLAN ID. This method implements seamless interworking between two user networks.

VLAN IDs in two directly connected Layer 2 networks are different because of different plans. The user needs to manage the two networks as a single Layer 2 network. For example, Layer 2 connectivity and Layer 2 protocols need to be deployed uniformly.

VLAN mapping can be configured on the switch connecting the two user networks to map VLAN IDs on the two user networks. This implements Layer 2 connectivity and uniform management.

Principle Description

After receiving a single tagged packet, the switch determines to replace a single tag based on the VLAN mapping mode. Then the switch learns the MAC addresses contained in the packet. Based on the source MAC address and mapped VLAN ID, the switch updates the MAC address entries in the VLAN mapping table. Based on the destination MAC address and the mapped VLAN ID, the switch searches for the MAC address entries. If the destination MAC address matches no entry, the switch broadcasts the packet in the specified VLAN; if the destination MAC address matches an entry, the switch forwards the packet through the corresponding outbound interface.

2.6.2 Configuration

Configuring VLAN Mapping

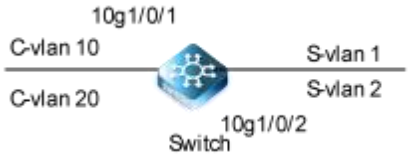


Figure 2-10 vlan-mapping

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the vlan configure mode and create vlan

```
switch(config)#vlan 1,2,10,20
switch(config)# exit
```

step 3 enable interface mapped vlan

```
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#vlan-mapping enable
```

step 4 Configure the vlan mapping table

```
switch(config-10ge1/0/1)#vlan-mapping vlan 10 map-vlan 1
switch(config-10ge1/0/1)#vlan-mapping vlan 20 map-vlan 2
switch(config-10ge1/0/1)#exit
```

step 5 Exit the configure mode

```
switch(config)# end
```

step 6 Validation

Use the following command to display the information of the switch port interface:

```
switch(config-10ge1/0/1)#show
!
interface 10gigaethernet 1/0/1
 vlan-mapping enable
 vlan-mapping vlan 10 map-vlan 1
 vlan-mapping vlan 20 map-vlan 2
```

Use the following command to display the information of the vlan mapping table：

```
switch(config)#show vlan-mapping

  Support Max Interface Number      :64
  Support Max Map List Number       :2048
  Current Map List Number           :2
  Interface          In-VID   Out-VID   Out-802.1p  Map-InVID   Map-In802.1p      Map-OutVID   Map-Out802.1p
  10ge1/0/1          --       10/10     --          --          --                1            --
  10ge1/0/1          --       20/20     --          --          --                2            --

Map-OutVID   Map-Out802.1p
1            --
2            --
```

2.7 Configuring MVRP

2.7.1 Overview

Function Introduction

Multiple VLAN Registration Protocol (MVRP) is a Layer 2 messaging protocol that manages the addition, deletion, and renaming of active virtual LANs, thereby reducing network administrators' time spent on these tasks. Using MVRP means that you do not have to manually register VLANs on all connections—that is, you do not need to explicitly bind a VLAN to each trunk interface. With MVRP, you configure a VLAN on one interface and the VLAN configuration is distributed through all active interfaces in the domain.The primary purpose of MVRP is to manage dynamic VLAN registration in Layer 2 networks. In managing dynamic VLAN registration, MVRP also prunes VLAN information.

MVRP is an Layer 2 application protocol of the Multiple Registration Protocol (MRP) and is defined in the IEEE 802.1ak standard. MRP and MVRP were designed by IEEE to perform the same functions as Generic Attribute Registration Protocol (GARP) and GARP VLAN Registration Protocol (GVRP) while overcoming some GARP and GVRP limitations, in particular, limitations involving bandwidth usage and convergence time in large networks with large numbers of VLANs.

MVRP was created by IEEE as a replacement application for GVRP. MVRP and GVRP cannot be run concurrently to share VLAN information in a Layer 2 network.

Principle Description

N/A

2.7.2 Configuration

Dynamic VLAN Registration

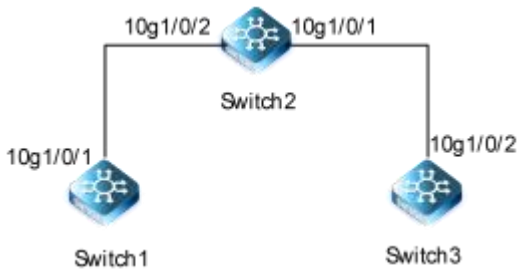


Figure 2-18 Dynamic VLAN Registration

Sw1,Sw2,Sw3 are configured as follows :

step 1 Enter the configure mode,and enable MVRP function

```
switch# configure
switch(config)#mvrp start
```

step 2 Enter the interface configure mode, and enable MVRP function

```
switch1:
switch(config)#interface 10g 1/0/1
switch(config-10ge1/0/1)#mvrp enable

switch2:
switch(config)#interface 10g 1/0/1
switch(config-10ge1/0/2)#mvrp enable
switch(config-10ge1/0/1)#mvrp enable

switch3:
switch(config)#interface 10g 1/0/2
switch(config-10ge1/0/2)#mvrp enable
```

step 3 Enter the interface configure mode, and enable MVRP function

```
switch1:
switch(config)#interface 10g 1/0/1
switch(config-10ge1/0/1)#port link-type trunk
switch(config-10ge1/0/1)#port trunk allow-pass vlan all

switch2:
switch(config)#interface 10g 1/0/1
switch(config-10ge1/0/2)#port link-type trunk
switch(config-10ge1/0/2)#port trunk allow-pass vlan all
switch(config-10ge1/0/1)#port link-type trunk
```

```
switch(config-10ge1/0/1)#port trunk allow-pass vlan all


switch3:
switch(config)#interface 10g 1/0/2
switch(config-10ge1/0/2)#port link-type trunk
switch(config-10ge1/0/2)#port trunk allow-pass vlan all
```

step 4 Validation

VLAN 10 is created on Switch1, and VLAN 10 is created dynamically on other devices.

```
Switch1(config)#show mvrp
 Version                    : MVRP_VX2.10.00.00
 Compliance-GVRP            : disable
 Interface       JoinTime(ms)    LeaveTime(ms)    LeaveAllTime(ms)    PeriodicTime(ms)    Mode        State
 10ge1/0/1       6000            30000            120000              N/A                 normal      enable
```

2.7.3 Application cases

N/A

2.8 Configuring Link Aggregation

2.8.1 Overview

Function Introduction

This chapter contains a sample configuration of Link Aggregation Control Protocol (LACP) . LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregation is viewed as a single link to each switch. The spanning tree views it as one interface. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption. This implementation supports the aggregation of maximum 16 physical Ethernet links into a single logical channel. LACP enables our device to manage link aggregation group between other devices that conform to the 802.3ad protocol. By using the LACP, the switch learns the identity of partners supporting LACP and the capabilities of each port. It then dynamically groups ports with same properties into a single logical bundle link.

Reference to standard IEEE 802.3ad.

Principle Description

N/A

2.8.2 Configuration

Link Aggregation in Manual Load Balancing Mode

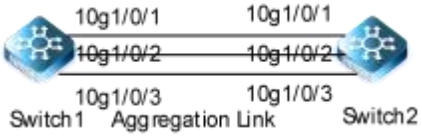


Figure 2-13 LACP

The configurations of Switch1 and Switch2 are as below:

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode

```
switch(config-eth-trunk1)#mode lacp-static
switch(config-eth-trunk1)#add 10gigaethernet 1/0/1
switch(config-eth-trunk1)#add 10gigaethernet 1/0/2
switch(config-eth-trunk1)#add 10gigaethernet 1/0/3
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

Use the following command to display the information of the trunk port :

```
switch(config)#show interface eth-trunk verbose
 Unknown-unicast-Alg:srcdst-mac

 Interface eth-trunk1:
  Schedule-Alg:src-mac
  Interface Mode:manual
  Port-List:
    Interface                 State(a/o)      InUtil          OutUtil
    10gigaethernet1/0/3       up/down         0.00%           0.00%
    10gigaethernet1/0/2       up/down         0.00%           0.00%
    10gigaethernet1/0/1       up/down         0.00%           0.00%
  Max-BW:(M):30000
  Cur-BW:(M):0
```

Use the following command to display the information of the LACP system:

```
switch(config)#show lacp system
 LACP system information:
        Max AG number: 32
        System Priority: 2000
        System MAC Address: 68:21:5f:b2:9c:be
        Fast Periodic Time: 1(s)
        Slow Periodic Time: 30(s)
        Short Timeout Time: 3(s)
        Long Timeout Time: 90(s)
```

```
        Churn Detection Time: 60(s)
        Join Ag waiting time: 2(s)
```

Link Aggregation in LACP Mode

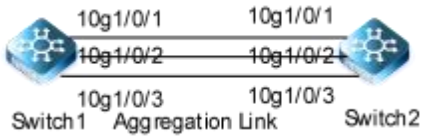


Figure 2-14 Lacp -stactic

The configurations of Switch1 and Switch2 are as below:

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode and add the interface to the channel group

```
switch(config-eth-trunk1)#mode lacp-static
switch(config-eth-trunk1)#add 10gigaethernet 1/0/1
switch(config-eth-trunk1)#add 10gigaethernet 1/0/2
switch(config-eth-trunk1)#add 10gigaethernet 1/0/3
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

Use the following command to display the configuration information of lacp:

```
switch(config)#show lacp config
!
lacp system-priority 2000
!
interface 10gigaethernet 1/0/1
!
interface 10gigaethernet 1/0/2
!
interface 10gigaethernet 1/0/3
!
interface eth-trunk 1
 mode lacp-static
```

Use the following command to display the information of the trunk port:

```
switch(config)#show lacp eth-trunk
  Interface        Status     PortNum    MainPort      MaxActiveIfNum
  eth-trunk1       master     3          ------        8
```

2.8.3 Application cases

N/A

2.9 Configuring M-LAG

2.9.1 Overview

Function Introduction

A multi-chassis link aggregation group (MLAG) is a type of link aggregation group (LAG) with constituent ports that terminate on separate chassis, primarily for the purpose of providing redundancy in the event one of the chassis fails.

Principle Description

N/A

2.9.2 Configuration

Configuring M-LAG

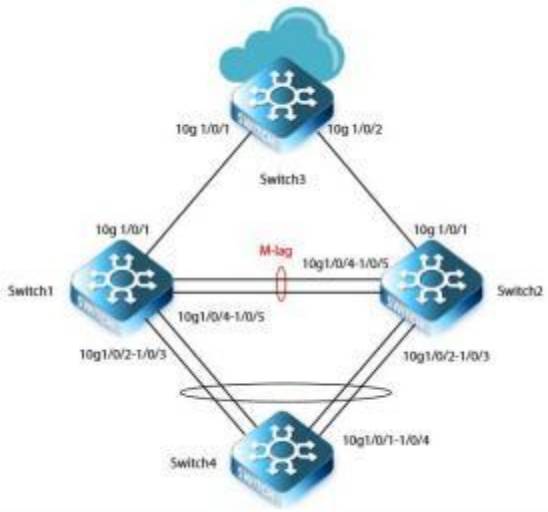


Figure 2-15 M-LAG

the switch4 is dual-homed to the IP network through M-LAG

step 1 Enter the configure mode

```
switch# configure
```

step 2 Bind the interface to an Eth-Trunk

Switch1

```
Sw1(config)#int eth-trunk 1
Sw1(config-eth-trunk1)#add 10gigaethernet 1/0/4
Sw1(config-eth-trunk1)#add 10gigaethernet 1/0/5
Sw1(config-eth-trunk1)#exit

Sw1(config)#int eth-trunk 2
Sw1(config-eth-trunk2)#add 10gigaethernet 1/0/2
Sw1(config-eth-trunk2)#add 10gigaethernet 1/0/3
Sw1(config-eth-trunk2)#exit
```

Switch2

```
Sw2(config)#int eth-trunk 1
Sw2(config-eth-trunk1)#add 10gigaethernet 1/0/4
Sw2(config-eth-trunk1)#add 10gigaethernet 1/0/5
Sw2(config-eth-trunk1)#exit

Sw2(config)#int eth-trunk 2
Sw2(config-eth-trunk2)#add 10gigaethernet 1/0/2
Sw2(config-eth-trunk2)#add 10gigaethernet 1/0/3
Sw2(config-eth-trunk2)#exit
```

step 3 Configuring the source IP address of DAD detection

Switch1

```
Sw1(config)#vlan 10
Sw1(vlan-10)#interface vlan 10
Sw1(vlan-vlanif-10)#ip address 10.1.1.1/24
Sw1(vlan-vlanif-10)#interface 10gigaethernet 1/0/1
Sw1(config-10ge1/0/1)#port hybrid vlan 10 tagged
Sw1(config-10ge1/0/1)#exit
```

Switch2

```
Sw2(config)#vlan 10
Sw2(vlan-10)#interface vlan 10
Sw2(vlan-vlanif-10)#ip address 10.1.1.2/24
Sw2(vlan-vlanif-10)#interface 10gigaethernet 1/0/1
Sw2(config-10ge1/0/1)#port hybrid vlan 10 tagged
Sw2(config-10ge1/0/1)#exit
```

step 4 Configuring M-LAG interface

Switch1

```
Sw1(config)#mlag-group 1
Sw1(config-mlag-1)#peerlink interface eth-trunk 1
Sw1(config-mlag-1)#mlag 1 interface eth-trunk 2
Sw1(config-mlag-1)#source-address 10.1.1.1 peer address 10.1.1.2
Sw1(config-mlag-1)#dad enhance enable Sw1(config-mlag-1)#exit
Sw1(config)#mlag exclude int 10gigaethernet 1/0/1
```

Switch2

```
Sw2(config)#mlag-group 1
Sw2(config-mlag-1)#peerlink interface eth-trunk 1
Sw2(config-mlag-1)#mlag 1 interface eth-trunk 2
Sw2(config-mlag-1)#source-address 10.1.1.2 peer address 10.1.1.1
Sw2(config-mlag-1)#dad enhance enable Sw2(config-mlag-1)#exit
Sw2(config)#mlag exclude int 10gigaethernet 1/0/1
```

step 5 Configuring V-STP

Switch1

```
Sw1(config)#stp
Sw1(config-stp)#stp tc-flush-arp enable
Sw1(config-stp)#stp v-stp enable
Sw1(config-stp)#stp flush disable
```

Switch2

```
Sw2(config)#stp
Sw2(config-stp)#stp tc-flush-arp enable
Sw2(config-stp)#stp v-stp enable
Sw2(config-stp)#stp flush disable
```

Step 6 Configuring Mlink

Switch1

```
Sw1(config)#mlink group 1
Sw1(config)#int eth-trunk 2
Sw1(config-eth-trunk2)#join mlink group 1 role downlink

Sw1(config-eth-trunk2)#interface 10gigaethernet 1/0/1
Sw1(config- 10ge1/0/1)#join mlink group 1 role uplink
Sw1(config- 10ge1/0/1)#exit
```

Switch2

```
Sw2(config)#Mlink group 1
Sw2(config)#int eth-trunk 2
Sw2(config-eth-trunk2)#join mlink group 1 role downlink

Sw2(config-eth-trunk2)#interface 10gigaethernet 1/0/1
```

```
Sw2(config- 10ge1/0/1)#join mlink group 1 role uplink
Sw2(config- 10ge1/0/1)#exit
```

Step 7 Configuring the layer 3 interface on downlink interface

Switch1

```
Sw1(config)#vlan 100
Sw1(vlan-100)#interface vlan 100
Sw1(config-vlanif-100)#ip address 100.1.1.1/24
Sw1(config-vlanif-100)#mac address 00:01:01:01:01:10
Sw1(config-vlanif-100)#int eth-trunk 2
Sw1(config-eth-trunk2)#port hybrid vlan 100 tagged
```

Switch2

```
Sw2(config)#vlan 100
Sw2(vlan-100)#interface vlan 100
Sw2(config-vlanif-100)#ip address 100.1.1.1/24
Sw2(config-vlanif-100)#mac address 00:01:01:01:01:10
Sw2(config-vlanif-100)#int eth-trunk 2
Sw2(config-eth-trunk2)#port hybrid vlan 100 tagged
```

2.10 Configuring Flow Control

2.10.1Overview

Function Introduction

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When the local device detects any congestion at its end, it can notify the link partner or the remote device of the congestion by sending a pause frame. You can use the flow control interface configuration command to set the interface's ability to receive and send pause frames to on, off. The default state for ports is receive off and send off. In auto-negotiation link, local device’s flow control ability can be notified to link partner by link up/down.

Note ： Flow control send/receive on ability only works on full duplex link

Principle Description

N/A

2.10.2 Configuration

Configuring Flow Control

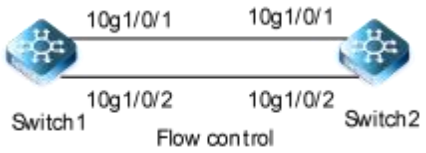


Figure 2-16 Flow control

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode and enable flowcontrol send

```
switch(config)#interface 10g 1/0/1
switch(config-10ge1/0/1)#flow-control enable
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

Use the following command to display the information configuration under the port:

```
switch(config-10ge1/0/1)#show
!
interface 10gigaethernet 1/0/1
 flow-control enable
```

2.10.3 Application cases

N/A

2.11 Configuring Storm Control

2.11.1 Overview

Function Introduction

Storm control refers to limiting the received maximum broadcast, maximum unknown multicast and maximum unknown unicast traffic on the specified interface to prevent flooding from consuming too much switch resources and ensure the normal operation of the business.Storm control can be done in one of two ways:

- Percent mode.

- package rate model(cir).

Principle Description

N/A

2.11.2 Configuration

Configuring Bandwidth Percentage Storm Control

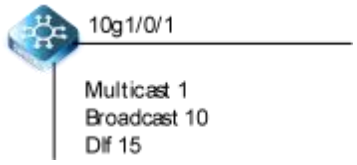


Figure 2-17 Percentage Storm Control

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode, and Set the percentage of storm control

```
switch(config)#interface 10g 1/0/1
switch(config-10ge1/0/1)#storm-control multicast percent 1
switch(config-10ge1/0/1)#storm-control broadcast percent 10
switch(config-10ge1/0/1)#storm-control dlf percent 15
```

step 3 Exit the configure mode

```
switch(config-10ge1/0/1)#end
```

step 4 Validation

```
switch(config)#show storm-control interface 10g 1/0/1
Interface       Type          Status   Limit    Mode       CIR(bps)        CBS(btyes)
10ge1/0/1       multicast     enable   1        percent    0               0
10ge1/0/1       broadcast     enable   10       percent    0               0
10ge1/0/1       dlf           enable   15       percent    0               0
```

Configuring storm control using package rate mode

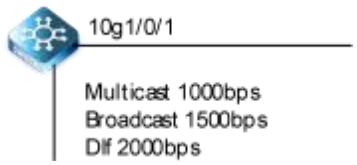


Figure 2-18 Cir Storm Control

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode, and set the storm control pps

Unknown unicast, multicast, and broadcast messages can be set respectively:

```
switch(config)#interface 10g 1/0/1
switch(config-10ge1/0/1)#storm-control multicast cir mbps 1000 cbs bytes 10000
switch(config-10ge1/0/1)#storm-control broadcast cir mbps 1500 cbs bytes 10000
switch(config-10ge1/0/1)#storm-control dlf cir mbps 2000 cbs bytes 10000
```

step 3 Exit the configure mode

```
switch(config-10ge1/0/1)#end
```

step 4 Validation

```
switch(config-10ge1/0/1)#show storm-control interface
Interface       Type          Status   Limit      Mode       CIR(bps)        CBS(btyes)
10ge1/0/1       multicast     enable   0          bps        1G              10000
10ge1/0/1       broadcast     enable   0          bps        1500M           10000
```

2.11.3 Application cases

N/A

2.12 MSTP Configuration

2.12.1 overview

Function Introduction

The MSTP (Multiple Spanning Tree Algorithm and Protocol (IEEE 802.1Q-2005)) enables multiple VLANs to be mapped to the same spanning-tree instance, thereby reducing the number of spanning-tree instances needed to support a large number of VLANs. The MSTP provides for multiple forwarding paths for data traffic and enables load balancing. It improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths). The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network; this deployment provides the highly-available network required in a service-provider environment. When the switch is in the multiple spanning-tree (MST) modes, the Rapid Spanning Tree Protocol (RSTP), which is based on IEEE 802.1w, is automatically enabled. The RSTP provides rapid convergence of the spanning tree through explicit handshaking that eliminates the IEEE 802.1D forwarding delay and quickly transitions root ports and designated ports to the forwarding state.

Principle Description

N/A

2.12.2 Configuration

Configuring Basic MSTP Functions

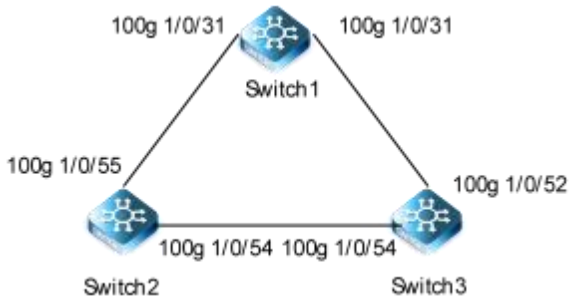


Figure 2-19 MSTP

The configurations of Switch-Switch2 are as blow. The configurations of these 3 Switches are same if there is no special description.

step 1 Enter the configure mode

```
switch#configure
```

step 2 Configuring the mode of MSTP

```
switch(config)#stp
switch(config-stp)#stp mode mstp
switch(config-stp)#quit
```

step 3 Enter the vlan configure mode and create vlan

```
switch(config)#vlan 1000-1001
```

step 4 Enter the MSTP configure mode，create region and instance. Bind the vlan to the instance.

```
switch(config)#stp
switch(config-stp)#stp instance 1 vlan 1000
switch(config-stp)#stp instance 2 vlan 1001
switch(config-stp)#quit
```

step 5 Configure MSTP priority and enable STP on different devices

Switch:

```
switch(config)#stp
switch(config-stp)#stp instance 1 priority 0
switch(config-stp)#quit
switch(config)#int 100g 1/0/31
```

```
switch(config-100ge1/0/31)#stp enable
switch(config-100ge1/0/31)#int 100g 1/0/27
switch(config-100ge1/0/27)#stp enable
switch(config-100ge1/0/27)#quit
```

Switch1:

```
switch1(config)#stp
switch1(config-stp)#stp instance 2 priority 0
switch1(config-stp)#int 100g 1/0/52
switch1(config-100ge1/0/52)#stp enable
switch1(config-100ge1/0/52)#int 100g 1/0/54
switch1(config-100ge1/0/54)#stp enable
switch1(config-100ge1/0/54)#quit
```

Switch2:

```
switch2(config)#int 100g 1/0/55
switch2(config-100ge1/0/55)#stp enable
switch2(config-100ge1/0/55)#int 100g 1/0/54
switch2(config-100ge1/0/54)#stp enable
switch2(config-100ge1/0/54)#quit
Switch(config)# spanning-tree enable
```

step 6 Enter the interface configure mode, and set the switch port mode and bind to the vlan

```
switch(config)#int 100g 1/0/27
switch(config-100ge1/0/27)#port hybrid vlan 1000-1001 tagged
switch(config-100ge1/0/27)#int 100g 1/0/31
switch(config-100ge1/0/31)#port hybrid vlan 1000-1001 tagged
switch(config-100ge1/0/31)#quit
```

step 7 Exit the configure mode

```
switch(config)# end
```

step 8 Validation

Use the following command to display the information of MSTP on Switch:

```
switch#show stp brief
MSTID Port                Role           STP State      Protection      Region
0     100ge1/0/27         root           forward        N/A             same
0     100ge1/0/31         alternate      discarding     N/A             same
1     100ge1/0/27         designated     forward        N/A             same
1     100ge1/0/31         designated     forward        N/A             same
2     100ge1/0/27         root           forward        N/A             same
2     100ge1/0/31         alternate      discarding     N/A             same
```

Use the following command to display the information of MSTP on Switch1:

```
switch1#show stp brief
MSTID Port            Role          STP State     Protection    Region
0     100ge1/0/52     designated    forward       N/A           same
0     100ge1/0/54     designated    forward       N/A           same
1     100ge1/0/52     root          forward       N/A           same
1     100ge1/0/54     designated    forward       N/A           same
2     100ge1/0/52     designated    forward       N/A           same
2     100ge1/0/54     designated    forward       N/A           same
```

Use the following command to display the information of MSTP on Switch2:

```
switch2#show stp brief
MSTID Port            Role          STP State     Protection    Region
0     100ge1/0/54     root          forward       N/A           same
0     100ge1/0/55     designated    forward       N/A           same
1     100ge1/0/54     alternate     discarding    N/A           same
1     100ge1/0/55     root          forward       N/A           same
2     100ge1/0/54     root          forward       N/A           same
2     100ge1/0/55     designated    forward       N/A           same
```

2.12.3 Application cases

N/A

3 IP Service Configuration Guide

3.1 ARP Configuration

3.1.1 Overview

Function Introduction

The Address Resolution Protocol (ARP) is a protocol used to dynamically map between Internet host addresses and Ethernet addresses. ARP caches Internet-Ethernet address mappings. When an interface requests a mapping for an address not in the cache, ARP queues the message, which requires the mapping, and broadcasts a message on the associated network requesting the address mapping. If a response is provided, the new mapping is cached and any pending message is transmitted. ARP will queue at most one packet while waiting for a response to a mapping request; only the most recently transmitted packet is kept. If the target host does not respond after 3 requests, the host is considered to be down, allowing an error to be returned to transmission attempts during this interval. If a target host does not send message for a period (normally one hour), the host is considered to be uncertainty, and several requests (normally 6, 3 unicast and 3 broadcast) will send to the host before delete the ARP entry. ARP entries may be added, deleted or changed manually. Manually added entries may be temporary or permanent.

Principle Description

N/A

3.1.2 Configuration

Configuring ARP

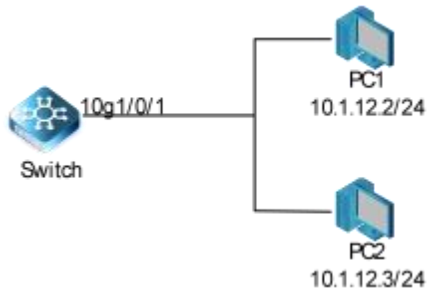


Figure 3-1 arp

In this configuration example, interface 100g1/0/1 assigned with address 10.1.12.1/24, on subnet10.1.12.0/24, there are two hosts, and their IP addresses are 10.1.12.2, 10.1.12.3, MAC address are 001a-a011-eca2, 001a-a011-eca3. ARP entry of host 10.1.12.2 is added manually, the entry of host 10.1.12.3 is added dynamically. Time-out period of ARP entries for interface eth-0-1 configure to 20 minutes.

step 1 Enter the configure mode

step 2 Configuring the layer 3 interface and set the ip address

```
switch1(config)#vlan 10
switch1(vlan-10)#int vlan 10
switch1(config-vlanif-10)#ip add 10.1.12.1/24
switch1(config)#int    100g 1/0/1
```

```
switch1(config-100ge1/0/1)#port link-type access
switch1(config-100ge1/0/1)#port default vlan 10
```

step 3 Configuring arp aging timeout value and the arp retry interval value

```
Switch(config-vlanif-10)# ip arp aging-time 1200
Switch(config-vlanif-10)# exit
```

step 4 Add a static arp entry

```
Switch(config)# ip arp 10.1.12.2 01:1a:a0:11:ec:a3
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

Use the following command to display the information of the arp entry:

```
switch1(config)#show ip arp
  Arp aging time: 1200(s)
  Destination      Mac-addr              Type      Aging     Vlan     Interface            Vpn-instance
  ------------------------------------------------------------------------------------------
  10.1.12.2        5453:2541:1221        static    never     N/A      N/A
  ------------------------------------------------------------------------------------------
  Total: 1         Dynamic: 0            Static: 1         Other: 0
```

3.1.3 Application cases

N/A

3.2 Configuring ARP Proxy

3.2.1 Overview

Function Introduction

Proxy ARP, the most common method for learning about other routes, enables an Ethernet host with no routing information to communicate with hosts on other networks or subnets. The host assumes that all hosts are on the same local Ethernet and that they can use ARP to determine their MAC addresses. If a switch receives an ARP request for a host that is not on the same network as the sender, the switch evaluates whether it has the best route to that host. If it does, it sends an ARP reply packet with its own Ethernet MAC address, and the host that sent the request sends the packet to the switch, which forwards it to the intended host. Proxy ARP treats all networks as if they are local and performs ARP requests for every IP address. Proxy ARP can be separated to 2 parts: Proxy ARP and local Proxy ARP. Local Proxy ARP is always used in the topology where the Device is enabled port isolate but still need to do communicating via routing. Internet Control Message Protocol (ICMP) redirects are disabled on interfaces where the local proxy ARP feature is enabled.

Principle Description

N/A

3.2.2 Configuration

Configuring ARP Proxy

Figure 3-2 arp proxy

As seen in the above topology, PC1 is belonged to VLAN10 and PC2 is belonged to VLAN20. If ARP proxy feature is not enabled, then PC1 and PC2 can not communicate with each other. As following, these steps are shown to enable ARP proxy feature for both VLAN interface 10 and VLAN interface 20.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the vlan configure mode and create vlan

```
switch(config)# vlan 10,20
```

step 3 Enter the interface configure mode, set the switch port mode and bind to the vlan

```
switch(config)# interface 100g1/0/1
switch(config-100ge1/0/1)# port link-type access
switch(config-100ge1/0/1)# port default vlan 10
switch(config-100ge1/0/1)# exit

switch(config)# interface 100g 1/0/2
switch(config-100ge1/0/2)# port link-type access
switch(config-100ge1/0/2)# port default vlan 20
switch(config-100ge1/0/2)# exit
```

step 4 Create the vlan interface, configure the ip address, and enable arp proxy

```
switch(config)# interface vlan 10
switch(config-vlanif-10)# ip address 192.168.1.1/24
switch(config-vlanif-10)# arp-proxy enable
switch(config-vlanif-10)# exit

switch(config)# interface vlan 20
switch(config-vlanif-10)# ip address 192.168.2.1/24
```

```
switch(config-vlanif-10)# arp-proxy enable
switch(config-vlanif-10)# exit
```

step 5 Exit the configure mode

```
switch(config)# end
```

step 6 Validation

Use the following command to display the information of the arp proxy configuration on the switch:

```
switch# show interface vlan config
!
interface vlan 10
 ip address 192.168.1.1/24
 arp-proxy enable
!
interface vlan 20
 ip address 192.168.2.1/24
 arp-proxy enable
```

3.2.3 Application cases

N/A

3.3 Configuring DHCP Client

3.3.1 Overview

Function Introduction

Dynamic Host Configuration Protocol(DHCP) client can acquire IP address and configuration dynamically from DHCP server by DHCP. If client and server is on the same physical subnet, client can communicate with server directly, otherwise they need DHCP relay agent which is used to forward DHCP messages. DHCP client can request IP address from DHCP server by broadcasting DHCP messages. After received IP address and lease correspond to it, client will configure itself and set the expired time. When half past the lease, client will sent DHCP messages for a new lease to use the IP address continually. If it success, DHCP client will renew the lease.

Principle Description

N/A

3.3.2 Configuration

Configuring DHCP Client

Figure 3-4 DHCP client

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode

```
switch(config)#vlan 1000
switch(vlan-1000)#int 100g 1/0/54
switch(config-100ge1/0/54)#port link-type access
switch(config-100ge1/0/54)#port default vlan 1000
switch(config-100ge1/0/54)#quit
```

step 3 Vlanif interface enable DHCP client

```
switch(config)#int vlan 1000
switch(config-vlanif-1000)#ip address dhcp enable
switch(config-vlanif-1000)#quit
```

step 4 Exit the configure mode

```
Switch(config-if)# end
```

step 5 Validation

Check interface configuration:

```
switch# configure
switch(config)#int vlan 1000
switch(config-vlanif-1000)#show
!
interface vlan 1000
 ip address dhcp enable
!
```

Check all DHCP client status:

```
switch(config)#show dhcp client
Dhcp client information:
Version:DHCPCLIENT_VB3.00.05.00
Interface:vlan1000
    Current state.....:Bound
    AllocatedIP......:100.1.1.2
    SubnetMask.......:255.255.255.0
    ServerIP.........:100.1.1.1
    Allocated lease...:180 seconds
    Lease T1 time.....:90 seconds
    Lease T2 time.....:157 seconds
    Lease Obtained....:2000/06/05    Mon   02:17:15
```

```
Lease timeout..... .....
:2000/06/05 Mon 02:20:15 Transaction ID
:0x1da317 Client ID..... :01
68 21 5f b7 5b 10
DNS.....:
Getway.....:
Domain.....:
```

Show DHCP client statistics:

```
switch(config)#show dhcp client statistic
Dhcp client statistic :
Interface number:vlan1000
  Packet total      Out number      :37
  Arp               Out number      :3
  Discover          Out number      :14
  Request           Out number      :20
  Decline           Out number      :0
  Release           Out number      :0
  Inform            Out number      :0
  Error dhcp        Out number      :0
  Error Arp         Out number      :0
  Packet total      In number       :21
  Offer             In number       :1
  Ack               In number       :20
  Nak               In number       :0
  Arp               In number       :0
  Error dhcp        In number       :0
  Error Arp         In number       :0
```

3.3.3 Application cases

N/A

3.4 Configuring DHCP Relay

3.4.1 Overview

Function Introduction

DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagram are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway address (girder field of the DHCP packet) and, if configured, adds the relay agent information option (option82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

Principle Description

N/A

3.4.2 Configuration

Configuring DHCP Relay

Figure 3-5 DHCP client

This figure is the networking topology for testing DHCP relay functions. We need two computers and one Switch to construct the test bed.Switch as a DHCP relay agent.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure Vlan

```
switch(config)#vlan 1000-1001
switch(config)#int 100g 1/0/31
switch(config-100ge1/0/31)#port hybrid vlan 1000 tagged
switch(config-100ge1/0/31)#int 100g 1/0/27
switch(config-100ge1/0/27)#port hybrid vlan 1001 tagged
```

step 3 Create vlanif, configure IP, and declare to OSPF

```
switch(config)#int vlan 1000
switch(config-vlanif-1000)#ip address 100.1.1.2/24
switch(config-vlanif-1000)#int vlan 1001
switch(config-vlanif-1001)#ip address 101.1.1.1/24

switch(config-vlanif-1001)#router ospf
switch(config-ospf-1)#router-id 2.2.2.2
switch(config-ospf-1)#network 100.1.1.0 255.255.255.0 area 0
switch(config-ospf-1)#network 101.1.1.0 255.255.255.0 area 0
switch(config-ospf-1)#quit
```

step 4 Interface enable DHCP relay

```
switch(config-vlanif-1001)#ip dhcp relay
```

step 5 Interface configure server-ip

```
switch(config-vlanif-1001)#dhcp   relay server-ip 100.1.1.1
switch(config-vlanif-1001)#quit
```

step 6 Validation

Check the interface configuration

```
switch(config)#int 100g 1/0/27
switch(config-100ge1/0/27)#show
!
interface 100gigaethernet 1/0/27
 port hybrid vlan 1000-1001 tagged

switch(config-100ge1/0/27)#int 100g 1/0/31
switch(config-100ge1/0/31)#show
!
interface 100gigaethernet 1/0/31
 no port hybrid vlan 1
 port hybrid vlan 1000-1001 tagged

switch(config-100ge1/0/31)#int vlan 1000
switch(config-vlanif-1000)#show
!
interface vlan 1000
 ip address 100.1.1.2/24

switch(config-vlanif-1000)#int vlan 1001
switch(config-vlanif-1001)#show
!
interface vlan 1001
 ip address 101.1.1.1/24
 ip dhcp relay
 dhcp relay server-ip 100.1.1.1
switch(config-vlanif-1001)#
```

Check the dhcp relay statistic

```
switch(config)#show dhcp relay statistic
Bad Packets In : 0
Packets In From Clients : 3
Discover In : 2
Request In : 1
Inform In : 0
Decline In : 0
Release In : 0
Packets In From Server : 2
```

```
Offer In : 1
ACK In : 1
NAK In : 0
Packets Out To Server : 3
Packets Out To Client : 2
Unicast Out To Client : 0
Broadcast Out To Client : 2
Packets Error Out : 0
BootReply Packets Drop : 0
BootRequest Packets Drop : 0
```

3.4.3 Application cases

N/A

3.5 Configuring DHCP server

3.5.1 Overview

Function Introduction

A DHCP server is an Internet host that returns configuration parameters to DHCP clients 。 DHCP server can provide IP address and network configuration for DHCP client by DHCP. For provide DHCP service， DHCP server need to be configured first. For example, IP address pool need be create , default gateway should be set in a pool, and some network parameters for DHCP client should be set before DHCP working. After DHCP server start to work, it will find a valid IP address from pool for DHCP client when receiving client's request. Meantime it also send network configuration parameters to client. The IP address assigned by DHCP server have a period of validity(lease), so DHCP client need to renew its lease before the lease expired for reserving current IP address by sending DHCP REQUEST message.

If DHCP server was in the same subnet with client,it can normal work after connect to subnet. Otherwise DHCP relay was needed for server providing DHCP service ,which can help to forward DHCP message between server and client.

Principle Description

N/A

3.5.2 Configuration

Configuring DHCP server

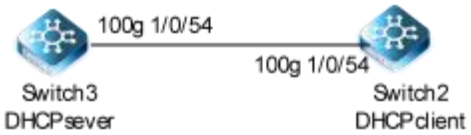


Figure 3-6 DHCP server

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enable DHCP server globally,configure the ip address pool

Configure Switch 3.

```
switch3(config)#dhcp start
switch3(config)#dhcp pool 2
switch3(config-dhcp-pool-2)#network 100.1.1.1 mask 255.255.255.0
switch3(config-dhcp-pool-2)#lease-time day 0 hour 0 minute 10
switch3(config-dhcp-pool-2)#quit
```

step 3 Enter the interface configure mode， set the attributes and ip address

Configure Switch 3.

```
switch3(config)#vlan 1000
switch3(config)#int 100g 1/0/54
switch3(config-100ge1/0/54)#port link-type access
switch3(config-100ge1/0/54)#port default vlan 1000
switch3(config-100ge1/0/54)#int vlan 1000
switch3(config-vlanif-1000)#ip address 100.1.1.1/24
switch3(config-vlanif-1000)#ip dhcp server
switch3(config-vlanif-1000)#quit
```

Configure Switch 2.

```
switch2(config)#vlan 1000
switch2(vlan-1000)#int 100g 1/0/54
switch2(config-100ge1/0/54)#port link-type access
switch2(config-100ge1/0/54)#port default vlan 1000
switch2(config-100ge1/0/54)#int vlan 1000
```

step 4 Validation

Check DHCP Server(switch3) status：

```
switch3#show running-config
!
dhcp start
dhcp relay hand disable
dhcp pool 2
 network range 100.1.1.1 100.1.1.254 mask 255.255.255.0
 lease-time day 0 hour 0 minute 3
!
!
interface vlan 1000
 ip address 100.1.1.1/24
 ip dhcp server
!
!
```

```
interface 100gigaethernet 1/0/54
 port link-type access
 port default vlan 1000
!
```

Check DHCP Client(switch2) ：

```
switch2(config-vlanif-1000)#show dh client
Dhcp client information:
Version:DHCPCLIENT_VB3.00.05.00
Interface:vlan1000
    Current state.....:Bound
    AllocatedIP......:100.1.1.4
    SubnetMask.......:255.255.255.0
    ServerIP.........:100.1.1.1
    Allocated lease...:180 seconds
    Lease T1 time.....:90 seconds
    Lease T2 time.....:157 seconds
    Lease Obtained....:2000/06/05 Mon 19:18:33
    Lease timeout....:2000/06/05 Mon 19:21:33
    Transaction ID....:0x61f13b
    Client ID.........:01 68 21 5f b7 5b 10
    DNS.............:
    Getway..........:
    Domain..........:
    Lease time will time out in 0 days 0 hours 02 minutes 50 seconds.
```

Check DHCP server statistics on DHCP Server(switch3):

```
switch3(config)#show dhcp server statistic
Pool Number : 2
Auto-bind IP Address Number : 1
Manual-bind IP Address Number : 0
Boot Request In: 3443
Discover In : 3411
Request In : 32
Decline In : 0
Release In :0
Boot Reply Out: 2811
Offer Out : 2779
ACK Out : 32
NAK Out : 0
Packets Error Out : 0
```

Check DHCP server addresses and interfaces on DHCP Server(switch3):

```
switch3(config)#show dhcp bind-entry

dhcp bind-entry number:1
```

Vpn-instance	IP	MAC	ExpireTime(seconds)	Type	ArpFlag
public	101.1.1.4	6821:5fb7:5b10	74	dynamic:temporary	no

Configuring DHCP server with relay

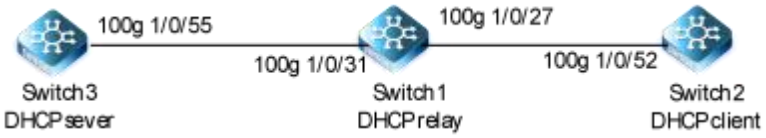


Figure 3-7 DHCP relay

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure the DHCP server

Configure Switch 3.

```
switch3(config)#vlan 1000
switch3(config)#int 100g 1/0/55
switch3(config-100ge1/0/55)#po hybrid   vlan 1000 tagged
switch3(config-100ge1/0/55)#quit
switch3(config)#int vlan 1000
switch3(config-vlanif-1000)#ip address 100.1.1.1/24
switch3(config-vlanif-1000)#ip dhcp server
switch3(config-vlanif-1000)#quit
```

Enable DHCP and configure address pool.

```
switch3(config)#dhcp start
switch3(config)#dhcp pool 1
switch3(config-dhcp-pool-1)#network 101.1.1.1 mask 255.255.255.0
switch3(config-dhcp-pool-1)#gateway 100.1.1.2
switch3(config-dhcp-pool-1)#lease-time day   0 hour 0 minute 4
switch3(config-dhcp-pool-1)#int vlan 1000
```

step 3 Configure the DHCP relay

Configure Switch 1.

```
switch1(config)#vlan 1000-1001
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#port hybrid   vlan 1000 tagged
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port hybrid   vlan 1001 tagged
switch1(config-100ge1/0/27)#quit
```

```
switch1(config)#int vlan 1000
switch1(config-vlanif-1000)#ip address 100.1.1.2/24
switch1(config-vlanif-1000)#int vlan 1001
switch1(config-vlanif-1001)#ip address 101.1.1.1/24
switch1(config-vlanif-1001)#quit
```

Configure DHCP relay.

```
switch1(config)#int vlan 1001
switch1(config-vlanif-1001)#ip dhcp  relay
switch1(config-vlanif-1001)#dhcp relay server-ip 100.1.1.1
switch1(config-vlanif-1001)#quit
```

step 4 Configure the DHCP client

Configure Switch 2.

```
switch2(config)#vlan 1001
switch2(vlan-1001)#int 100g 1/0/52
switch2(config-100ge1/0/52)#port hybrid vlan 1001 tagged
switch2(config-100ge1/0/52)#int vlan 1001
switch2(config-vlanif-1001)#ip address dhcp enable
```

step 5 Configure the OSPF

Configure DHCP Sever (Switch3).

```
switch3(config)#router ospf
switch3(config-ospf-1)#router-id 1.1.1.1
```

Configure DHCP Sever (Switch2).

```
switch1(config)#router ospf
switch1(config-ospf-1)#router-id 2.2.2.2
switch1(config-ospf-1)#network 100.1.1.0 255.255.255.0 area 0
switch1(config-ospf-1)#network 101.1.1.0 255.255.255.0 area 0
```

step 6 Validation

Check DHCP Server(Switch3) configuration:

```
switch3(config)#show running-config
!
dhcp start
dhcp relay hand disable
dhcp pool 1
 network range 101.1.1.1 101.1.1.254 mask 255.255.255.0
 gateway 100.1.1.2
 lease-time day 0 hour 0 minute 4
!
```

Check DHCP client status on DHCP Server(Switch2):

```
switch2(config)#show dhcp client
Dhcp client information:
Version:DHCPCLIENT_VB3.00.05.00
Interface:vlan1001
    Current state.....:Bound
    AllocatedIP......:101.1.1.4
    SubnetMask.......:255.255.255.0
    ServerIP.........:100.1.1.1
    Allocated lease...:180 seconds
    Lease T1 time.....:90 seconds
    Lease T2 time.....:157 seconds
    Lease Obtained....:2000/06/05 Mon 20:50:06
    Lease timeout....:2000/06/05 Mon 20:53:06
    Transaction ID....:0x173307
    Client ID........:01 68 21 5f b7 5b 10
    DNS.............:
    Getway..........:100.1.1.2
    Domain..........:
    Lease time will time out in 0 days 0 hours 01 minutes 55 seconds.
```

Check DHCP server statistics on DHCP Server(Switch2):

```
switch3(config)#show dhcp server statistic
Pool Number : 2
Auto-bind IP Address Number : 1
Manual-bind IP Address Number : 0
Boot Request In: 3507
Discover In : 3415
Request In : 92
Decline In : 0
Release In :0
Boot Reply Out: 2875
Offer Out : 2783
ACK Out : 92
NAK Out : 0
Packets Error Out : 0
```

Check DHCP server addresses and interfaces on DHCP Server(Switch3):

```
switch3(config)#show dhcp bind-entry

dhcp bind-entry number:1
 Vpn-instance                IP              MAC                ExpireTime(seconds)  Type                  ArpFlag
 public                      101.1.1.4       6821:5fb7:5b10     102                  dynamic:committed     no
```

3.5.3 Application cases

N/A

4 IP Routing Configuration Guide

4.1 Configuring IP Unicast-Routing

4.1.1 Overview

Function Introduction

Static routing is a special type of routing that is manually configured by an administrator.When the network structure is relatively simple, the configuration of static routing can make the network work normally.Proper configuration and use of static routing can improve network performance and ensure bandwidth for important network applications.The disadvantage of static routing is that when the network fails or the topology changes, the route may not be reachable, resulting in network outage.It is up to the network administrator to manually modify the configuration of the static route.

Static routing is useful in small networks and provides a simple solution to make several destinations accessible.Dynamic routing protocols are recommended for large networks.

Static routing consists of a network prefix (host address) and the next hop (gateway).

Principle Description

N/A

4.1.2 Configuration

Configuring static route

Figure 4-1 ip unicast routing

This example shows how to enable static route in a simple network topology.

There are 3 static routes on Switch1， one is to achieve remote network 10.10.12.0/24, the other two are to achieve the loopback addresses on Switch2 and Switch3. There is a default static route on Switch3, that is, static routes use same gateway or nexthop address. There are 2 static routes on swithc2, both of them are to achieve the remote switch's loopback address.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode，set the attributes and ip address

Configure on Switch1:

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.1/24
```

```
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10

Switch(config)# interface loopback 1
Switch(config-loopback-1)# ip address 10.1.1.1/32
Switch(config-loopback-1)# exit
```

Configure on Switch2:

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.2/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
switch(config)#vlan 20
switch(vlan-10)#quit
switch(config)#int vlan 20
switch(config-vlanif-20)#ip address 10.1.23.2/24
switch(config-vlanif-20)#quit
switch(config)#int 100g 1/0/2
switch(config-100ge1/0/2)#port link-type access
switch(config-100ge1/0/2)#port default vlan 20

Switch(config)# interface loopback 1
Switch(config-loopback-1)# ip address 20.1.1.1/32
Switch(config-loopback-1)# exit
```

Configure on Switch3:

```
switch(config)#vlan 20
switch(vlan-10)#quit
switch(config)#int vlan 20
switch(config-vlanif-20)#ip address 10.1.23.3/24
switch(config-vlanif-20)#quit
switch(config)#int 100g 1/0/2
switch(config-100ge1/0/2)#port link-type access
switch(config-100ge1/0/2)#port default vlan 20

Switch(config)# interface loopback 1
Switch(config-loopback-1)# ip address 30.1.1.1/32
Switch(config-loopback-1)# exit
```

step 3 Configuring static route

Configure on Switch1:

Note:Specify the destination prefix and mask for the network for which a gateway is required, for example, 10.10.12.0/24. Add a gateway for each of them (in this case 10.10.10.2 for all). Since R2 is the only next hop available, you can configure a default route instead of configuring the same static route for individual addresses.

```
switch(config)# ip route-static 10.1.23.0 255.255.255.0 10.1.12.2
switch(config)# ip route-static 20.1.1.1 255.255.255.255 10.1.12.2
switch(config)# ip route-static 30.1.1.1 255.255.255.255 10.1.12.2
```

Configure on switch2:

```
switch(config)# ip route-static 10.1.1.1 255.255.255.255 10.1.12.1
switch(config)# ip route-static 30.1.1.1 255.255.255.255 10.1.23.3
```

Configure on switch3:

Note:specify 10.10.12.2 as a default gateway to reach any network. since 10.10.12.2 is the only route available you can specify it as the default gateway instead of specifying it as the gateway for individual network or host addresses.

```
switch(config)# ip route-static 0.0.0.0 0.0.0.0 10.1.23.2
```

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

Use the following command to display the route information on switch1:

```
switch# show ip route
  Routing Tables: Public
  Destination          Gateway          Preference/Metric      Interface          Proto    Mpls    Vpn-Instance
  ------------------------------------------------------------------------------------------------------------

  10.1.1.1/32          1.1.1.1                0/1              loopback1          local    no      N/A
  10.1.23.0/24         10.1.12.2              60/60            vlan10             static no        N/A

  20.1.1.1/32          10.1.12.2              60/60            vlan10             static no        N/A
  30.1.1.1/32          10.1.12.2              60/60            vlan10             static no        N/A
  127.0.0.1/32         127.0.0.1              0/1              loopback0          local    no      N/A
  ------------------------------------------------------------------------------------------------------------

  Total: 5             static: 4              Down: 0
```

4.1.3 Application cases

N/A

4.2 Configuring RIP

4.2.1 Overview

Function Introduction

RIP (Routing Information Protocol) is a relatively simple Interior Gateway Protocol (IGP), which is mainly used in small scale networks.

RIP is a protocol based on distance-vector algorithm, which exchanges routing information through UDP packets.RIP USES Hop Count to measure the distance to the destination address, called RoutingCost.In RIP, the number of hops from a router to a network directly connected to it is 0, the number of hops from a network accessible through a router is 1, and so on.To limit the convergence time, RIP specifies that cost is an integer between 0 and 15, and the number of hops where COST is greater than or equal to 16 is defined as infinite, that is, the destination network or host cannot be reached.

To improve performance and prevent routing rings, RIP supports Split Horizon.RIP can also introduce routes obtained by other routing protocols.

Principle Description

Reference to RFC 2453

4.2.2 Configuration

Enabling RIP

Figure 4-2 enable rip

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode, set the attributes and ip address

Configure on switch1:

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.1/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
```

```
switch(config)# interface loopback 1
switch(config-loopback-1)# ip address 10.1.1.1/32
switch(config-loopback-1)# exit
```

Configure on switch2:

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.2/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
switch(config)#vlan 20
switch(vlan-10)#quit
switch(config)#int vlan 20
switch(config-vlanif-20)#ip address 10.1.23.2/24
switch(config-vlanif-20)#quit
switch(config)#int 100g 1/0/2
switch(config-100ge1/0/2)#port link-type access
switch(config-100ge1/0/2)#port default vlan 20



switch(config)# interface loopback 1
switch(config-loopback-1)# ip address 20.1.1.1/32
switch(config-loopback-1)# exit
```

Configure on switch3:

```
switch(config)#vlan 20
switch(vlan-10)#quit
switch(config)#int vlan 20
switch(config-vlanif-20)#ip address 10.1.23.3/24
switch(config-vlanif-20)#quit
switch(config)#int 100g 1/0/2
switch(config-100ge1/0/2)#port link-type access
switch(config-100ge1/0/2)#port default vlan 20



switch(config)# interface loopback 1
switch(config-loopback-1)# ip address 30.1.1.1/32
switch(config-loopback-1)# exit
```

step 3 Enable RIP routing process and associate networks

Configure on switch1:

```
switch(config)# router rip
switch(config-rip-1)#network 10.0.0.0/24
switch(config-rip-1)# exit
```

Configure on switch2:

```
switch(config)# router rip
switch(config-rip-1)#network 10.0.0.0/24
switch(config-rip-1)#network 20.0.0.0/24
switch(config-rip-1)# exit
```

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

Use the following command to display the database of rip on switch1:

```
switch# show ip rip interface

 Process                 :1
 Interface               :loopback1
 status                  :Up
 Passive Mode            :False
 Adress                  :10.1.1.1
 Netmask                 :255.255.255.255
 Authtication Type       :no authtication
 send Version            :rip version 1 compatible
 Receive Version         :rip version 1 or version 2
 Metric In               :0
 Metric Out              :1
 Default Metric          :1
 Md5 Compatible          :disable
 Packer Transmit Interval :200
 Packer Transmit Number  :20
 Bfd                     :disable

 Process                 :1
 Interface               :vlan20
 Status                  :Down
 Passive Mode            :False
 Adress                  :10.1.11.1
 Netmask                 :255.255.255.0
 Authtication Type       :no authtication
```

```
Send Version                    :rip version 1 compatible
Receive Version                 :rip version 1 or version 2
Metric In                       :0
Metric Out                      :1
Default Metric                  :1
Md5 Compatible                  :disable
Packer Transmit Interval        :200
Packer Transmit Number          :20
Bfd                             :disable

Process                         :1
Interface                       :vlan10
Status                          :Up
Passive Mode                    :False
Adress                          :10.1.12.1
Netmask                         :255.255.255.0
Authtication Type               :no authtication
Send Version                    :rip version 1 compatible
Receive Version                 :rip version 1 or version 2
Metric In                       :0
Metric Out                      :1
Default Metric                  :1
Md5 Compatible                  :disable
Packer Transmit Interval        :200
Packer Transmit Number          :20
Bfd                             :disable
```

Use the following command to display routes on Switch1:

```
switch# show ip route
  Routing Tables: Public
  Destination        Gateway          Preference/Metric    Interface          Proto   Mpls   Vpn-Instance
  ------------------------------------------------------------------------------------------------------
  10.1.1.1/32        10.1.1.1               0/1            loopback1          local   no     N/A
  10.1.12.0/24       10.1.12.1              0 / 1          vlan10             local   no     N/A
  10.1.12.0/24       10.1.12.1              100/1          vlan10             rip     no     N/A
  10.1.12.1/32       10.1.12.1              0 / 1          vlan10             local   no     N/A
  10.1.23.0/24       10.1.12.1              100/1          vlan10             rip     no     N/A
  20.1.1.1/32        10.1.12.1              100/1          vlan10             rip     no     N/A
  127.0.0.1/32       127.0.0.1              0/1            loopback0          local   no     N/A
  172.0.0.0/8        10.32.133.254          60/60          mgt-eth0/0/0       static  no     N/A
  ------------------------------------------------------------------------------------------------------
  Total: 11          Static: 2              Down: 0
```

Configuring Split-horizon Parameters

Figure 4-3 rip split-horizon

Normally,routers connected to a broadcast network and using the distance vector routing protocol use a horizontal partitioning mechanism to avoid loops.Configuration level splitting can prevent routes learned from one interface from being published outward through that interface, which generally optimizes communication between multiple routers, especially if the link is broken.

Configuring toxicity reversals allows routes learned from an interface to be published from that interface, but the measures for these routes are set to 16, which is unreachable.

step 1 precondition The above 4.3 configuration

step 2 Enabling debug on Switch2 (optional)

```
Switch# debug rip all
Switch# terminal monitor
```

step 3 Enter the configure mode

The following commands operate on Switch2:

```
Switch# configure
```

step 4 Enter the interface configure mode and set split-horizon

Disable Split-horizon:

```
Switch(config)#router rip
Switch(config-rip-1)# split-horizon disable
```

Enable Split-horizon and poisoned:

```
Switch(config-rip-1)# poison-reverse enable
Switch(config-rip-1)# split-horizon enable
```

step 5 Exit the configure mode

```
Switch(config-router)# end
```

step 6 Validation

Use the following command to display the configuration:

```
Switch(config-rip-1)#show
```

```
!
router rip 1
 poison-reverse enable
 network 10.0.0.0
 network 30.0.0.0
```

4.3 Configuring OSPF

4.3.1 Overview

Function Introduction

The Open Shortest Path First (OSPF) protocol, developed by the Internet Engineering Task Force (IETF), is a link-state Interior Gateway Protocol (IGP).It supports IP subnetworking and tagging external routes.Version 2 (RFC2328) is currently in use, with the following features:

- Receives and sends packets in multicast mode to reduce load on routers that do not run OSPF.
- Supports Classless Inter-domain Routing (CIDR).
- Supports load balancing among equal-cost routes.
- Supports packet encryption.

The current system supports the following OSPF features:

- Definition of stub areas is supported: Routes learned through any IP routing protocol can be redistributed into another IP routing protocol. At the intradomain level, this means that OSPF can import routes learned through RIP. OSPF routes can also be exported into RIP.
- Plain text and MD5 authentication among neighboring routers within an area is supported: Configurable routing interface parameters include interface output cost, retransmission interval, interface transmit delay, router priority, router dead and hello intervals, and authentication key.
- Virtual links are not supported: Not-so-stubby-areas (NSSAs) per RFC 1587 are not supported now. OSPF typically requires coordination among many internal routers, area border routers (ABRs) connected to multiple areas, and autonomous system boundary routers (ASBRs). The minimum configuration would use all default parameter values, no authentication, and interfaces assigned to areas. If you customize your environment, you must ensure coordinated configuration of all routers.

Principle Description

Reference to RFC 2328

4.3.2 Configuration

Basic OSPF Parameters Configuration

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure the OSPF

```
Switch(config)# router ospf 1
Switch(config-ospf-1)# network 10.1.12.0 255.255.255.0 area 0
Switch(config-ospf-1)# quit
```

Note : use the following command to delete the routing process

```
Switch(config)# no router ospf 1
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

```
Switch# show ip ospf config
Version:OSPFV2_VB3.00.11.00
!
router ospf 1
 router-id 10.1.1.1
 network 10.1.12.0 255.255.255.0 area 0
```

Enabling OSPF on the interface

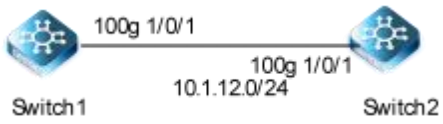


Figure 4-4 OSPF

This example shows the minimum configuration required for enabling OSPF on an interface.

Note： Configure one interface so that it belongs to only one area. However, you can configure different interfaces on a router to belong to different areas.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode, set the attributes and ip address

Configure Switch 1.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.1/24
switch(config-vlanif-10)#quit
```

```
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
```

Configure Switch 2.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.2/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
```

step 3 Configure the Routing process and associate the network with a specified OSPF area

Configure Switch 1.

```
Switch(config)# router ospf
Switch(config-ospf-1)# network 10.1.12.0 255.255.255.0 area 0
```

Configure Switch 2.

```
Switch(config)# router ospf
Switch(config-ospf-1)# network 10.1.12.0 255.255.255.0 area 0
```

Note: To using OSPF among two devices which are directly connected, the area IDs must be same. The ospf process IDs can be same or different.

step 4 Exit the configure mode

```
Switch(config-router)# end
```

step 5 Validation

Use the following command to display the neighbor of ospf:

Switch1.

```
Switch# show ip ospf neighbor
 OSPF Process 1
 IpAddress       NeighborID      Priority  State       Aging   UpTime      Interface
 10.1.12.2       10.1.12.2       1         full        35      0:00:35
```

Switch2.

```
Switch# show ip ospf neighbor
 OSPF Process 1
 IpAddress       NeighborID      Priority  State       Aging   UpTime      Interface
 10.1.12.1       10.1.12.1       1         full        33      e
```

Switch3.

```
Switch# show ip ospf route

OSPF Process 1
```

RoutType	Prefix	PathType	Cost	Cost2	NextHop	BackupNextHop	AreaId	Time
Network	10.1.12.0/24	INTRA	1	0	10.1.12.2	0.0.0.0	N/A	0:01:39

1.3.6 Configuring OSPF Area Parameters

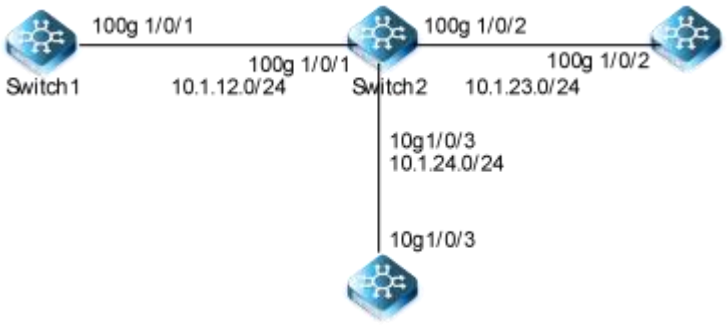


Figure 4-5 OSPF Area

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area and stub areas. Stub areas are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area for destinations outside the autonomous system (AS).

Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the area range router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode, set the attributes and ip address

Configure Switch 1.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.1/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
```

Configure Switch 2.

```
switch(config)#vlan 10
```

```
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.2/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
switch(config)#vlan 20
switch(vlan-10)#quit
switch(config)#int vlan 20
switch(config-vlanif-20)#ip address 10.1.23.2/24
switch(config-vlanif-20)#quit
switch(config)#int 100g 1/0/2
switch(config-100ge1/0/2)#port link-type access
switch(config-100ge1/0/2)#port default vlan 20
switch(config)#int vlan 30
switch(config-vlanif-30)#ip address 10.1.24.2/24
switch(config-vlanif-30)#quit
switch(config)#int 100g 1/0/3
switch(config-100ge1/0/3)#port link-type access
switch(config-100ge1/0/3)#port default vlan 30
```

Configure Switch3.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.23.3/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/2
switch(config-100ge1/0/2)#port link-type access
switch(config-100ge1/0/2)#port default vlan 10
```

Configure Switch 4.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.24.4/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
```

step 3 Configure the Routing process and associate the network with a specified OSPF area

Configure Switch 1.

```
Switch(config)# router ospf 1
```

```
Switch(config-ospf-1)# network 10.1.12.0 255.255.255.0 area 0
Switch(config-ospf-1)# quit
```

Configure Switch 2.

```
Switch(config)# router ospf 1
Switch(config-ospf-1)# network 10.1.12.0 255.255.255.0 area 0
Switch(config-ospf-1)# network 10.1.23.0 255.255.255.0 area 1
Switch(config-ospf-1)# network 10.1.24.0 255.255.255.0 area 2
Switch(config-ospf-1)# area 1 stub
Switch(config-ospf-1) #area 2 nssa
Switch(config-router)# quit
```

Configure Switch 3.

```
Switch(config)# router ospf 1
Switch(config-ospf-1)# network 10.1.23.0 255.255.255.0 area 1
Switch(config-router)# area 1 stub
Switch(config-router)# quit
```

Configure Switch 4.

```
Switch(config)# router ospf 1
Switch(config-ospf-1)# network 10.1.23.0 255.255.255.0 area 1
Switch(config-router)# area 1 stub
Switch(config-router)# quit
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

Use the following command to display the ospf routes:

Switch1：

```
Switch# show ip ospf route


 OSPF Process 1
 RoutType    Prefix          PathType  Cost   Cost2   NextHop      BackupNextHop     AreaId   Time
 ABR         20.1.1.1/32     INTRA     1      0       10.1.12.2    0.0.0.0           0        0:05:23
 ASBR        20.1.1.1/32     INTRA     1      0       10.1.12.2    0.0.0.0           0        0:05:23
 Network     10.1.12.0/24    INTRA     1      0       10.1.12.1    0.0.0.0           N/A      0:36:46
 Network     10.1.23.0/24    INTER     2      0       10.1.12.2    0.0.0.0           N/A      0:06:20
 Network 10.1.24.0/24        INTER     2      0       10.1.12.2    0.0.0.0           N/A      0:05:28
```

Switch2：

```
Switch# show ip ospf route


 OSPF Process 1
```

RoutType	Prefix	PathType	Cost	Cost2	NextHop	BackupNextHop	AreaId	Time
Network	10.1.12.0/24	INTRA	1	0	10.1.12.2	0.0.0.0	N/A	0:37:35
Network	10.1.23.0/24	INTRA	1	0	10.1.23.2	0.0.0.0	N/A	0:03:30
Network	10.1.24.0/24	INTRA	1	0	10.1.24.4	0.0.0.0	N/A	0:06:15

Switch3：

```
Switch# show ip ospf route

 OSPF Process 1
```

RoutType	Prefix	PathType	Cost	Cost2	NextHop	BackupNextHop	AreaId	Time
ABR	20.1.1.1/32	INTRA	1	0	10.1.23.2	0.0.0.0	1	0:02:20
Network	0.0.0.0/0	INTER	1	0	10.1.23.2	0.0.0.0	N/A	0:02:20
Network	10.1.12.0/24	INTER	2	0	10.1.23.2	0.0.0.0	N/A	0:02:20
Network	10.1.23.0/24	INTRA	1	0	10.1.23.3	0.0.0.0	N/A	0:02:23
Network	10.1.24.0/24	INTER	2	0	10.1.23.2	0.0.0.0	N/A	0:02:20

Redistributing Routes into OSPF

Figure 4-6 OSPF Redistribute

In this example the configuration causes RIP routes to be imported into the OSPF routing table and advertised as Type 5 External LSAs into Area 0.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode, set the attributes and ip address

Configure Switch 1.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.1/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10

Switch(config)# interface loopback 1
Switch(config-loopback-1)# ip address 10.1.1.1/32
Switch(config-loopback-1)# exit
```

Configure Switch2.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.2/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
switch(config)#vlan 20
switch(vlan-10)#quit
switch(config)#int vlan 20
switch(config-vlanif-20)#ip address 10.1.23.2/24
switch(config-vlanif-20)#quit
switch(config)#int 100g 1/0/2
switch(config-100ge1/0/2)#port link-type access
switch(config-100ge1/0/2)#port default vlan 20
```

Configure Switch3.

```
switch(config)#vlan 20
switch(vlan-10)#quit
switch(config)#int vlan 20
switch(config-vlanif-20)#ip address 10.1.23.3/24
switch(config-vlanif-20)#quit
switch(config)#int 100g 1/0/2
switch(config-100ge1/0/2)#port link-type access
switch(config-100ge1/0/2)#port default vlan 20

Switch(config)# interface loopback 1
Switch(config-loopback-1)# ip address 30.1.1.1/32
Switch(config-loopback-1)# exit
```

step 3 Configure the Routing process and associate the network with a specified OSPF area

Configure Switch 1.

```
Switch(config)# router ospf 1
Switch(config-ospf-1)# network 10.1.12.0 255.255.255.0 area 0
Switch(config-ospf-1)# network 10.1.1.1 255.255.255.255 area 0
Switch(config-ospf-1)# quit
```

Configure Switch 2.

```
Switch(config)# router ospf 1
Switch(config-ospf-1)# network 10.1.12.0/24 area 0
Switch(config-ospf-1)# redistribute rip 1
Switch(config-ospf-1)# quit
```

step 4 Enable RIP routing process and associate networks

Configure Switch 2.

```
Switch(config)# router rip 1
Switch(config-rip-1)# network 10.10.10.0
Switch(config-rip-1)# redistribute rip
Switch(config-rip-1)# quit
```

Configure Switch 3.

```
Switch(config)# router rip 1
Switch(config-rip-1)# network 10.10.10.0
Switch(config-rip-1)# network 30.0.0.0
Switch(config-rip-1)# quit
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

Use the following command to display the ospf routes:

Switch1：

```
Switch# show ip ospf route

 OSPF Process 1
RoutType  Prefix          PathType  Cost  Cost2  NextHop     BackupNextHop  AreaId  Time
ASBR      20.1.1.1/32     INTRA     1     0      10.1.12.2   0.0.0.0        0       0:03:34
Network   10.1.1.1/32     INTRA     1     0      10.1.1.1    0.0.0.0        N/A     0:05:39
Network   10.1.12.0/24    INTRA     1     0      10.1.12.1   0.0.0.0        N/A     1:10:40
Network   10.1.23.0/24    ASE2      1     1      10.1.12.2   0.0.0.0        N/A     0:03:34
Network   30.1.1.1/32     ASE2      1     1      10.1.12.2   0.0.0.0        N/A     0:03:34
```

Switch2：

```
Switch# switch2#show ip ospf route

 OSPF Process 1
RoutType  Prefix          PathType  Cost  Cost2  NextHop     BackupNextHop  AreaId  Time
Network   10.1.1.1/32     INTRA     2     0      10.1.12.1   0.0.0.0        N/A     0:04:08
Network   10.1.12.0/24    INTRA     1     0      10.1.12.2   0.0.0.0        N/A     0:04:12
switch2#show ip rip database

 Rip Process : 1
 Total : 6
 Process  Destination  Netmask          Gateway     Metric Age  State  Proto  Tag
 1        10.1.1.1     255.255.255.255  10.1.12.1   1      0    ACTIVE ospf   0
```

1	10.1.12.0	255.255.255.0	10.1.12.2	0	0	ACTIVE rip	0
1	10.1.23.0	255.255.255.0	10.1.23.3	1	0	ACTIVE rip	0
1	10.1.23.0	255.255.255.0	10.1.23.2	0	0	ACTIVE rip	0
1	10.1.24.0	255.255.255.0	10.1.24.4	0	0	ACTIVE rip	0
1	30.1.1.1	255.255.255.255	10.1.23.3	1	0	ACTIVE rip	0

Switch3：

```
Switch# show ip rip database

Rip Process : 1
Total : 6
```

Process	Destination	Netmask	Gateway	Metric	Age	State	Proto	Tag
1	10.1.1.1	255.255.255.255	10.1.23.2	2	15	ACTIVE rip	0	
1	10.1.12.0	255.255.255.0	10.1.23.2	1	15	ACTIVE rip	0	
1	10.1.23.0	255.255.255.0	10.1.23.3	0	0	ACTIVE rip	0	
1	10.1.23.0	255.255.255.0	10.1.23.2	1	15	ACTIVE rip	0	
1	10.1.24.0	255.255.255.0	10.1.23.2	1	15	ACTIVE rip	0	
1	30.1.1.1	255.255.255.255	30.1.1.1	0	0	ACTIVE rip	0	

Configuring OSPF authentication

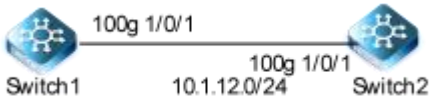


Figure 4-7 OSPF authentication

In our implementation there are three types of OSPF authentications--Null authentication (Type 0), Simple Text (Type 1) authentication and MD5 (Type 2) authentication. With null authentication, routing exchanges over the network are not authenticated. In Simple Text authentication, the authentication type is the same for all routers that communicate using OSPF in a network. For MD5 authentication, you configure a key and a key-id on each router. The router generates a message digest on the basis of the key, key ID and the OSPF packet and adds it to the OSPF packet.

The Authentication type can be configured on a per-interface basis or a per-area basis. Additionally, Interface and Area authentication can be used together. Area authentication is used for an area and interface authentication is used for a specific interface in the area. If the Interface authentication type is different from Area authentication type, Interface authentication type overrides the Area authentication type. If the Authentication type is not specified for an interface, the Authentication type for the area is used. The authentication command descriptions contain details of each type of authentication. Refer to the OSPF Command Reference for OSPF authentication commands.

The following example briefly introduces the three types of OSPF validation.No authentication is used between Switch1 and Switch2;Use plaintext authentication between Switch2 and Switch3;MD5 authentication is used between Switch3 and Switch4.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode, set the attributes and ip address. Set the ospf authentication under the interface configure mode

Configure Switch 1.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.1/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
```

Configure Switch 2.

```
switch(config)#vlan 10
switch(vlan-10)#quit
switch(config)#int vlan 10
switch(config-vlanif-10)#ip address 10.1.12.2/24
switch(config-vlanif-10)#quit
switch(config)#int 100g 1/0/1
switch(config-100ge1/0/1)#port link-type access
switch(config-100ge1/0/1)#port default vlan 10
```

step 3 Configure the Routing process and associate the network with a specified OSPF area

Configure Switch 1.

```
Switch(config)# router ospf
Switch(config-ospf-1)# network 10.1.12.0 255.255.255.0 area 0
```

Configure Switch 2.

```
Switch(config)# router ospf
Switch(config-ospf-1)# network 10.1.12.0 255.255.255.0 area 0
```

step 4 Exit the configure mode

```
Switch(config)# end
```

step 5 Configure area authentication under the OSPF process

Configure Switch 1.

```
Switch(config)# router ospf
Switch(config-ospf-1)# area 0 authentication md5 1 cipher 123
```

Configure Switch 2.

```
Switch(config)# router ospf
Switch(config-ospf-1)# area 0 authentication md5 1 cipher 123
```

step 6 Configure area authentication under the OSPF interface

Configure Switch 1.

```
switch(config)#int vlan 10
switch1(config-vlanif-10)#ip ospf authentication md5 1 cipher 123
```

Configure Switch 2.

```
switch(config)#int vlan 10
switch1(config-vlanif-10)#ip ospf authentication md5 1 cipher 123
```

step 7 Validation

Use the following command to display the neighbor of ospf:

Switch1：

```
Switch# show ip ospf neighbor
 OSPF Process 1
IpAddress        NeighborID      Priority  State      Aging   UpTime      Interface
10.1.12.2        10.1.12.2       1         full       35      0:00:35
```

Switch2：

```
Switch# show ip ospf neighbor
 OSPF Process 1
IpAddress        NeighborID      Priority  State      Aging   UpTime      Interface
10.1.12.1        10.1.12.1       1         full       33      0:01:07
```

4.3.3 Application cases

N/A

4.4 Configuring Prefix-list

4.4.1 Overview

Function Introduction

Routing Policy is the technology for modifying route information to change traffic route. Prefix list is a kind of route policies that used to control and modify routing information. A prefix list is identified by list name and contains one or more ordered entries which are processed sequentially. Each entry provides a matched range for network prefix and has a unique sequence number in the list. In the matching process， switch will check entries orderly. If a entry matches conditions, this process would finish.

Principle Description

N/A

4.4.2 Configuration

Basic Configuration

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Create a prefix-list

Note: Create a prefix-list. If the sequence of the rule is not specified, system should automatically assign an sequence number for it. Support different actions such as permit and deny. Support to add description string for a prefix-list.

```
Switch(config)# ip prefix-list 1 index 10 permit 10.1.12.0/24
Switch(config)# ip prefix-list 1 index 20 deny 10.1.23.0/24
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

Use the following command to display the prefix-list:

```
Switch# show ip prefix-list 1
ip prefix-list : 1
 index: 10        permit 10.1.12.0/24
 index: 20        deny      10.1.23.0/24
```

4.4.3 Application cases

N/A

4.5 Configuring Route-policy

4.5.1 Overview

Function Introduction

Routing Policy is a technology used to modify Routing information in order to change the path of network traffic. It is mainly realized by changing Routing attributes (including accessibility).

When routers publish and receive routing information, they may need to enforce policies to filter routing information, such as receiving or publishing only routing information that meets certain conditions.One routing protocol may need to introduce the routing information discovered by other routing protocols. When introducing the routing information of other routing protocols, the router may only need to introduce part of the routing information that meets the requirements of this protocol and control some properties of the introduced routing information to meet the requirements of this protocol.To implement a routing policy,

you first define the characteristics of the routing information that will enforce the routing policy, that is, define a set of matching rules.Different properties in routing information can be set as matching basis, such as destination address, router address where routing information is published, and so on.Matching rules can be set up in advance and then applied to the routing policy of the process of publishing, receiving, and introducing a route.

Principle Description

N/A

4.5.2 Configuration

Configuring Route-Policy to apply to OSPF

step 1 Enter the configure mode

```
Switch# configure
```

step 2Create routing policies and set rules and behavior

```
Switch(config)#route-policy 1 permit node 10
switch(config-route-policy)#match cost 100
switch(config-route-policy)#apply cost 10
switch(config-route-policy)#
```

step 3 enter the OSPF routing mode, redistribute the RIP protocol to OSPF, and use the policy

```
switch(config)#router ospf
switch(config-ospf-1)#red
switch(config-ospf-1)#redistribute rip rou
switch(config-ospf-1)#redistribute rip route-policy 1
```

step 4 Exit the configure mode

```
Switch(config)# end
```

step 5 Validation

```
Switch# show route-policy 1
policyName:1
    type:permit     node:10 (matched count 0)
   match cost 100
   apply cost 10
```

Configuring Route-Policy to apply to BGP

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create a list of IP prefixes

```
switch(config)# ip prefix-list 1 permit    10.1.1.1/32
```

step 3Create a routing policy, match the access control list rules, and set the behavior

```
Switch(config)# router-policy 1 permit node 10
Switch(config-route-policy)# match ip-prefix 1
Switch(config-route-policy)# apply local-preference 1000
Switch(config-route-policy)# exit
```

step 3 enter BGP routing mode and use the policy

```
switch(config)# router bgp 1
switch(config-bgp)# neighbor 10.1.12.2 remote-as 1
switch(config-bgp)# neighbor 10.1.12.2 router-policy 1 export
switch(config-bgp)# network 10.1.1.1/32
switch(config-bgp)# network 10.1.1.2/32
switch(config-bgp)# exit
```

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

```
Switch# show route-policy 1
policyName:1
    type:permit     node:10 (matched count 10)
   match ip-prefix 1
   apply local-preference 1000


    type:permit     node:20 (matched count 13)
Switch# show ip bgp route

Total 2 Routes
DestAddr/Prefixlen      Peer            Nexthop         Protocol  Med     LocalPrf  Origin  Vpn-
Instance    As-Path
10.1.1.1/32             10.1.12.1       10.1.12.1       bgp       0       1000      IGP     N/A
10.1.1.2/32             10.1.12.1       10.1.12.1       bgp       0       100       IGP     N/A
```

4.5.3 Application cases

N/A

4.6 Configuring BGP

4.6.1 Overview

Function Introduction

The Border Gateway Protocol (BGP) is an inter-Autonomous System routing protocol.

The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the list of Autonomous Systems (ASes) that reachability information traverses. This information is sufficient for constructing a graph of AS connectivity for this reachability, from which routing loops may be pruned and, at the AS level, some policy decisions may be enforced.

BGP-4 provides a set of mechanisms for supporting Classless Inter-Domain Routing (CIDR) [RFC1518, RFC1519]. These mechanisms include support for advertising a set of destinations as an IP prefix and eliminating the concept of network "class" within BGP. BGP-4 also introduces mechanisms that allow aggregation of routes, including aggregation of AS paths.

Routing information exchanged via BGP supports only the destination-based forwarding paradigm, which assumes that a router forwards a packet based solely on the destination address carried in the IP header of the packet. This, in turn, reflects the set of policy decisions that can (and cannot) be enforced using BGP. BGP can support only those policies conforming to the destination-based forwarding paradigm.

Principle Description

For more BGP information please reference [RFC 1771, RFC 4271].

4.6.2 Configuration

Configuring EBGP

Figure 4-8 EBGP

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode and set the attributes

Switch1:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
Switch(config-vlanif-10)#ip address 10.1.12.1/24
Switch(config-vlanif-10)#quit
Switch(config)#int 100g 1/0/1
```

```
Switch(config-100ge1/0/1)#port link-type access
Switch(config-100ge1/0/1)#port default vlan 10
Switch(config)int loopback 1
Switch(config-loopback-1)ip address 1.1.1.1/32
```

Switch2:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
Switch(config-vlanif-10)#ip address 10.1.12.2/24
Switch(config-vlanif-10)#quit
Switch(config)#int 100g 1/0/1
Switch(config-100ge1/0/1)#port link-type access
Switch(config-100ge1/0/1)#port default vlan 10

Switch(config)#vlan 20
Switch(vlan-10)#int vlan 20
Switch(config-vlanif-20)#ip address 10.1.23.2/24
Switch(config-vlanif-20)#quit
Switch(config)#int 100g 1/0/2
Switch(config-100ge1/0/2)#port link-type access
Switch(config-100ge1/0/2)#port default vlan 20
Switch(config)int loopback 1
Switch(config-loopback-1)ip address 2.2.2.2/32
```

Switch3:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
Switch(config-vlanif-10)#ip address 10.1.23.3/24
Switch(config-vlanif-10)#quit
Switch(config)#int 100g 1/0/2
Switch(config-100ge1/0/2)#port link-type access
Switch(config-100ge1/0/2)#port default vlan 10
Switch(config)int loopback 1
Switch(config-loopback-1)ip address 3.3.3.3/32
```

step 3 Configuring a ospf route

Switch1:

```
Switch(config)#router ospf
Switch(config-ospf-1)#network 10.1.12.0 255.255.255.0 area 0
Switch(config-ospf-1)#network 1.1.1.1 255.255.255.255 area 0
```

Switch2:

```
Switch(config)#router ospf
Switch(config-ospf-1)#network 10.1.12.0 255.255.255.0 area 0
Switch(config-ospf-1)#network 10.1.23.0 255.255.255.0 area 0
```

```
Switch(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
```

Switch2:

```
Switch(config)#router ospf
Switch(config-ospf-1)#network 10.1.23.0 255.255.255.0 area 0
Switch(config-ospf-1)#network 3.3.3.3 255.255.255.255 area 0
```

step 4 Configuring the Routing process and set the router id, set the neighbor, associate the network, and set the redistribute attributes

Switch1:

```
Switch(config)# router bgp 100
Switch(config-bgp)# router-id 1.1.1.1
Switch(config-bgp)# neighbor 10.1.12.2 remote-as 200
Switch(config-bgp)# network 1.1.1.1 255.255.255.255
```

Switch2:

```
Switch(config)# router bgp 200
Switch(config-bgp)# router-id 2.2.2.2
Switch(config-bgp)# neighbor 10.1.12.1 remote-as 100
Switch(config-bgp)# neighbor 10.1.23.3 remote-as 300
Switch(config-bgp)# exit
```

Switch3:

```
Switch(config)# router bgp 300
Switch(config-bgp)# router-id 3.3.3.3
Switch(config-bgp)# neighbor 10.1.23.2 remote-as 200
Switch(config-bgp)# exit
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

Switch2:

```
Switch(config-bgp)#show ip bgp neighbor


 BGP local router ID :2.2.2.2
 Local AS number :200
 Total number of neighbors :2                Neighbors in established state:2
 Neighbor                Version  AS         MsgIn      MsgOut     Up/Down      State       StateChange
VpnInstance
 10.1.12.1               4        100        4          4          00:01:11     Established 1           N/A
 10.1.23.3               4        300        4          4          00:01:02     Established 1           N/A
```

Configuring IBGP

Figure 4-9 IBGP

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode and set the attributes

Switch1:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
Switch(config-vlanif-10)#ip address 10.1.12.1/24
Switch(config-vlanif-10)#quit
Switch(config)#int 100g 1/0/1
Switch(config-100ge1/0/1)#port link-type access
Switch(config-100ge1/0/1)#port default vlan 10
Switch(config)int loopback 1
Switch(config-loopback-1)ip address 1.1.1.1/32
```

Switch2:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
Switch(config-vlanif-10)#ip address 10.1.12.2/24
Switch(config-vlanif-10)#quit
Switch(config)#int 100g 1/0/1
Switch(config-100ge1/0/1)#port link-type access
Switch(config-100ge1/0/1)#port default vlan 10

Switch(config)#vlan 20
Switch(vlan-10)#int vlan 20
Switch(config-vlanif-20)#ip address 10.1.23.2/24
Switch(config-vlanif-20)#quit
Switch(config)#int 100g 1/0/2
Switch(config-100ge1/0/2)#port link-type access
Switch(config-100ge1/0/2)#port default vlan 20
Switch(config)int loopback 1
Switch(config-loopback-1)ip address 2.2.2.2/32
```

Switch3:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
```

```
Switch(config-vlanif-10)#ip address 10.1.23.3/24
Switch(config-vlanif-10)#quit
Switch(config)#int 100g 1/0/2
Switch(config-100ge1/0/2)#port link-type access
Switch(config-100ge1/0/2)#port default vlan 10
Switch(config)int loopback 1
Switch(config-loopback-1)ip address 3.3.3.3/32
```

step 3 Configure a ospf route

Switch1:

```
Switch(config)#router ospf
Switch(config-ospf-1)#network 10.1.12.0 255.255.255.0 area 0
Switch(config-ospf-1)#network 1.1.1.1 255.255.255.255 area 0
```

Switch2:

```
Switch(config)#router ospf
Switch(config-ospf-1)#network 10.1.12.0 255.255.255.0 area 0
Switch(config-ospf-1)#network 10.1.23.0 255.255.255.0 area 0
Switch(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
```

Switch2:

```
Switch(config)#router ospf
Switch(config-ospf-1)#network 10.1.23.0 255.255.255.0 area 0
Switch(config-ospf-1)#network 3.3.3.3 255.255.255.255 area 0
```

step 4 Configure the Routing process and set the router id, set the neighbor, associate the network, and set the redistribute attributes

Switch1:

```
Switch(config)# router bgp 100
Switch(config-bgp)# router-id 1.1.1.1
Switch(config-bgp)# neighbor 1.1.1.1 remote-as 100
Switch(config-bgp)# neighbor 10.1.12.2 update-source
Switch(config-bgp)# network 1.1.1.1 255.255.255.255
```

Switch2:

```
Switch(config)# router bgp 100
Switch(config-bgp)# router-id 2.2.2.2
Switch(config-bgp)# neighbor 10.1.12.1 remote-as 100
Switch(config-bgp)# neighbor 10.1.23.3 remote-as 100
Switch(config-bgp)# exit
```

Switch3:

```
Switch(config)# router bgp 100
Switch(config-bgp)# router-id 3.3.3.3
Switch(config-bgp)# neighbor 10.1.23.2 remote-as 100
Switch(config-bgp)# exit
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

Switch2:

```
Switch(config-bgp)#show ip bgp neighbor


 BGP local router ID :2.2.2.2
 Local AS number :100
 Total number of neighbors :2                Neighbors in established state:2
 Neighbor                Version  AS         MsgIn     MsgOut    Up/Down      State       StateChange
VpnInstance
 10.1.12.1               4        100        4         4         00:01:11     Established 1           N/A
 10.1.23.3               4        100        4         4         00:01:02     Established 1           N/A
```

4.6.3 Application cases

N/A

4.7 Configuring ISIS

4.7.1 Overview

Function Introduction

IS-IS Routing Protocol, which may be used as an interior,gateway protocol (IGP) to support TCP/IP as well as OSI. This allowsa single routing protocol to be used to support pure IP environments,pure OSI environments, and dual environments. This specification wasdeveloped by the IS-IS working group of the Internet Engineering Task Force.

The OSI IS-IS protocol has reached a mature state, and is ready for implementation and operational use. The most recent version of the OSI IS-IS protocol is contained in ISO DP 10589 . The proposed standard for using IS-IS for support of TCP/IP will therefore make use of this version (with a minor bug correction, as discussed in Annex B). We expect that future versions of this proposed standard will upgrade to the final International Standard version of IS-IS when available.

Principle Description

For more BGP information please reference [RFC 1195]

4.7.2 Configuration

Configuring ISIS

Figure 4-10 ISIS

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode and set the attributes

Switch1:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
Switch(config-vlanif-10)#ip address 10.1.12.1/24
Switch(config-vlanif-10)#quit
Switch(config)#int 100g 1/0/1
Switch(config-100ge1/0/1)#port link-type access
Switch(config-100ge1/0/1)#port default vlan 10
```

Switch2:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
Switch(config-vlanif-10)#ip address 10.1.12.2/24
Switch(config-vlanif-10)#quit
Switch(config)#int 100g 1/0/1
Switch(config-100ge1/0/1)#port link-type access
Switch(config-100ge1/0/1)#port default vlan 10

Switch(config)#vlan 20
Switch(vlan-10)#int vlan 20
Switch(config-vlanif-20)#ip address 10.1.23.2/24
Switch(config-vlanif-20)#quit
Switch(config)#int 100g 1/0/2
Switch(config-100ge1/0/2)#port link-type access
Switch(config-100ge1/0/2)#port default vlan 20
```

Switch3:

```
Switch(config)#vlan 10
Switch(vlan-10)#int vlan 10
Switch(config-vlanif-10)#ip address 10.1.23.3/24
Switch(config-vlanif-10)#quit
```

```
Switch(config)#int 100g 1/0/2
Switch(config-100ge1/0/2)#port link-type access
Switch(config-100ge1/0/2)#port default vlan 10
```

step 3 Configure the isis process and enable the isis process under the interface

Switch1:

```
Switch(config)#router isis
Switch(config-isis-1)#is-type level-2
Switch(config-isis-1)#net 49.0001.0000.0000.0001.00
Switch(config)int vlan 10
Switch(config-vlanif-10)ip router isis
```

Switch2:

```
Switch(config)#router isis
Switch(config-isis-1)#is-type level-1-2
Switch(config-isis-1)#net 49.0002.0000.0000.0001.00
Switch(config)int vlan 10
Switch(config-vlanif-10)ip router isis
Switch(config-vlanif-10)exit
Switch(config)int vlan 20
Switch(config-vlanif-20)ip router isis
```

Switch3:

```
Switch(config)#router isis
Switch(config-isis-1)#is-type level-1
Switch(config-isis-1)#net 49.0002.0000.0000.0001.00
Switch(config)int vlan 10
Switch(config-vlanif-10)ip router isis
```

4.7.3 Application cases

N/A

5 Multicast Configuration Guide

5.1 Configuring IGMP

5.1.1 Overview

Function Introduction

To participate in IP multicasting, multicast hosts, routers, and multilayer switches must have the IGMP operating. This protocol defines the querier and host roles:

- A querier is a network device that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver that sends report messages (in response to query messages) to inform a querier of a host membership.
- A set of queries and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use IGMP messages to join and leave multicast groups. -- Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message. Membership in a multicast group is dynamic; hosts canjoin and leave at any time. There is no restriction on the location or number of members in a multicast group.

A host can be a member of more than one multicast group at a time. How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it can be very short-lived. Membership in a group can constantly change. A group that has members can have no activity.

IGMP packets are sent using these IP multicast group addresses:

- IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
- IGMP group-specific queries are destined to the group IP address for which the switch is querying.
- IGMP group membership reports are destined to the group IP address for which the switch is reporting.
- IGMP Version 2 (IGMPv2) leave messages are destined to the address 224.0.0.2.

Principle Description

Reference to RFC 1112，RFC 2236，RFC 3376

5.1.2 Configuration

There is no explicit command to enable IGMP, which is always combined with PIM-SM. When PIM-SM is enabled on an interface, IGMP will be enabled automatically on this interface, vice versa. But notice, before IGMP can work, IP Multicast-routing must be enabled globally firstly. We support build IGMP group record by learning IGMP packets or configuring static IGMP group by administrator.

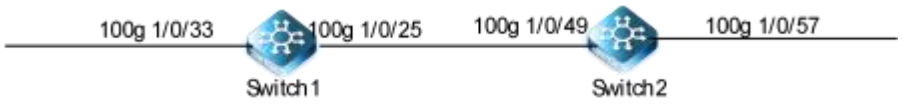


Figure 5-1 IGMP

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enable ip multicast-routing globally

```
switch(config)#ip multicast-routing
switch1(config)#igmp start
switch1(config)#igmp
```

step 3 Enter the interface configure mode，set the attributes and ip address

```
switch1(config)#interface 10gigaethernet 1/0/33
switch1(config-10ge1/0/33)# port link-type trunk
switch1(config-10ge1/0/33)# no port trunk allow-pass vlan 1
switch1(config-10ge1/0/33)# port trunk allow-pass vlan 400
switch1(config)#interface vlan 400
switch1(config-vlanif-400)# ip address 20.1.20.1/24

switch1(config)#interface 100gigaethernet 1/0/25
switch1(config-100ge1/0/25)# port link-type trunk
switch1(config-100ge1/0/25)# no port trunk allow-pass vlan 1
switch1(config-100ge1/0/25)# port trunk allow-pass vlan 300
switch1(config)#interface vlan 300
switch1(config-vlanif-300)# ip address 20.1.23.2/24

switch2(config)#interface 100gigaethernet 1/0/49
switch2(config-100ge1/0/49)# port link-type trunk
switch2(config-100ge1/0/49)# no port trunk allow-pass vlan 1
switch2(config-100ge1/0/49)# port trunk allow-pass vlan 300
switch2(config)#interface vlan 300
switch2(config-vlanif-300)# ip address 20.1.23.3/24

switch2(config)#interface 10gigaethernet 1/0/57
switch2(config-10ge1/0/57)# port link-type trunk
switch2(config-10ge1/0/57)# no port trunk allow-pass vlan 1
switch2(config-10ge1/0/57)# port trunk allow-pass vlan 500
switch2(config)#interface vlan 500
switch2(config-vlanif-500)# ip address 20.1.30.1/24
```

step 4 Globally enabled routing protocols, such as OSPF

```
switch1(config)#router ospf 5
switch1(config-ospf-5)# router-id 20.1.20.1
  WARNING:Changing the parameter in this command resets the neighbor session.Continue?(y/n) [y]y
switch1(config-ospf-5)# network 20.1.20.1 255.255.255.255 area 0
switch1(config-ospf-5)# network 20.1.23.2 255.255.255.255 area 0
```

```
switch2(config)#router ospf 5
switch2(config-ospf-5)# router-id 20.1.30.1
  WARNING:Changing the parameter in this command resets the neighbor session.Continue?(y/n) [y]y
switch2(config-ospf-5)# network 20.1.23.3 255.255.255.255 area 0
```

step 5 The interface enables PIM-SM and IGMP

```
switch(config)#interface vlan 400
switch(config-vlanif-400)# igmp enable
switch(config-vlanif-400)# ip pim-sm

switch(config)#interface vlan 300
switch(config-vlanif-300)# ip pim-sm
switch1(config-vlanif-300)# ip pim c-bsr group default
switch1(config-vlanif-300)# ip pim c-rp group default

switch2(config)#interface vlan 300
switch2(config-vlanif-300)# ip pim-sm

switch2(config)#interface vlan 500
switch2(config-vlanif-500)# igmp enable
switch2(config-vlanif-500)# ip pim-sm
```

step 6 Configure IGMP parameters on the interface (Optional)

```
switch(config)#interface vlan 400
switch(config-vlanif-400)# igmp version v3
switch(config-vlanif-400)# igmp max-response-time 20
switch(config-vlanif-400)# igmp timer query 60
switch(config-vlanif-400)# igmp robust-count 5
switch(config-vlanif-400)# igmp timer other-querier-present 310
switch(config-vlanif-400)# igmp lastmember-queryinterval 2
```

Step 7 Configure the maximum number of IGMP groups (Optional)

Global and interface can configure the number of IGMP groups:

```
switch1(config)# igmp
switch1(config-igmp)# limit 1000

switch1(config)#interface vlan 400
```

Step 8 Configure static IGMP groups

```
switch1(config)#interface vlan 400
switch1(config-vlanif-400)# igmp static-group 225.0.0.1 egress-port 10gigaethernet 1/0/3
```

step 9 Exit the configure mode

```
Switch(config)# end
```

step 10 Validation

Use the following command to display the information of igmp interfaces:

```
switch1(config)#show igmp config
!
igmp start
igmp
 limit 1000

 Interface vlan400
 igmp enable
 igmp version v3
 igmp limit 500
 igmp static-group 225.0.0.1 egress-port 10gigaethernet 1/0/33



switch1(config)#show igmp interface vlan 400
Interface vlan400
IGMP VPN Instance: Public
  IGMP Status: enable
  Require-router-alert: disable
  Send-router-alert: enable
  Timer Query: 125 s
  Robust-count: 2
  Max Response Time: 10 s
  Timer Other Querier Present: 255 s
  Last Member Query Interval: 1 s
  Version: v3
  Fast-leave: disable
  Querier Uptime: 119 s
  Wrong Version Querier: 0
  Joins: 0
  Groups: 1
  Last Listener Query Count: 2
  Startup Query Count: 0
  Startup Query Interval: 31 s
  Query Remain: 57 s
  Querier Address: 20.1.20.1
  SSM Mapping: disable
  IGMP Limit: 500
```

Use the following command to display IGMP group information:

```
switch1(config)#show igmp source all

 Interface        Group-Address    Source-Address   Expiry-Time      Mode      Status
 vlan400          225.0.0.1        0.0.0.0          0                include static

switch1(config)#show igmp egress-port all

 Interface        Group-Address    Source-Address   Egress-Port              Status
 vlan400          225.0.0.1        0.0.0.0          10ge1/0/33               static

switch1(config)#show igmp group

 Vpn Instance:Public
 Interface:vlan400
  Group Address:225.0.0.1
  Last Reporter Address:0.0.0.0
  Uptime:2000/01/02  21:16:58
  Expiry Time:0 s
```

5.1.3 Application cases

N/A

5.2 Configuring PIM-SM

5.2.1 Overview

Function Introduction

The Protocol Independent Multicasting-Sparse Mode (PIM-SM) is a multicast routing protocol designed to operate efficiently across Wide Area Networks (WANs) with sparsely distributed groups. It helps network nodes that are geographically dispersed to conserve bandwidth, and reduces traffic by simultaneously delivering a single stream of information to multiple locations.

PIM-SM uses the IP multicast model of receiver-initiated membership, supporting both shared and shortest-path trees, and uses soft-state mechanisms to adapt to changing network conditions. It relies on a topology-gathering protocol to populate a multicast routing table with routes.

Principle Description

The PIM-SM module is based on the following IETF standard: RFC 4601

The following is a brief description of the PIM-SM protocol:

- **Rendezvous Point (RP)：** An RP is responsible for processing Register messsages from the multicast source and Join messages from group members. All PIM routers on the network know the position of the RP. An RP can serve multiple multicast groups simultaneously, but each multicast group can be associated with only one RP.

- **Multicast Routing Information Base (MRIB)：** The MRIB is a multicast topology table derived from the unicast routing table. In PIM-SM, the MRIB is used to decide where to send Join/Prune messages. It also provides routing metrics for destination addresses. These metrics are used when sending and processing Assert messages.

- **Reverse Path Forwarding：** Reverse Path Forwarding (RPF) is a concept of an optimized form of flooding, where the router accepts a packet from SourceA through Interface IF1 only if IF1 is the interface the router would use in order to reach SourceA. It determines whether the interface is correct by consulting its unicast routing tables. The packet that arrives through interface IF1 is forwarded because the routing table lists this interface as the shortest path to the network. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link once in each direction.

- **Tree Information Base (TIB)：** The TIB is the collection of state at a PIM router storing the state of all multicast distribution trees at that router. It is created by receiving Join/Prune messages, Assert messages, and IGMP information from local hosts.

- **Upstream：** Towards to root of the tree. The root of the tree might be either the Source or the RP.

- **Downstream：** Away from the root of the tree. The root of tree might be either the Source or the RP.

- **Source-Based Trees：** In the Source-Based Trees concept, the forwarding paths are based on the shortest unicast path to the source. If the unicast routing metric is hop counts, the branches of the multicast Source-Based Trees are minimum hop. If the metric is delay, the branches are minimum delay. For every multicast source, there is a corresponding multicast tree that directly connects the source to all receivers. All traffic to the members of an associated group passes along the tree made for their source. Source-Based Trees have two entries with a list of outgoing interfaces-- the source address and the multicast group.

- **Shared Trees：** Shared trees or RP trees (RPT) rely on a central router called the Rendezvous Point (RP) that receives all traffic from the sources, and forwards that traffic to the receivers. All hosts might not be receivers. There is a single tree for each multicast group, regardless of the number of sources. Only the routers on the tree know about the group, and information is sent only to interested receivers. With an RP, receivers have a place to join, even if no source exists. The shared tree is unidirectional, and information flows only from the RP to the receivers. If a host other than the RP has to send data on the tree, the data must first be tunneled to the RP, and then multicast to the members. This means that even if a receiver is also a source, it can only use the tree to receive packets from the RP, and not to send packets to the RP (unless the source is located between the RP and the receivers).

- **Bootstrap Router (BSR)：** When a new multicast sender starts sending data packets, or a new receiver starts sending the Join message towards the RP for that multicast group, it needs to know the next-hop router towards the RP. The BSR provides group-to-RP mapping information to all the PIM routers in a domain, allowing them to map to the correct RP address.

- **Sending out Hello Messages：** PIM routers periodically send Hello messages to discover neighboring PIM routers. Hello messages are multicast using the address 224.0.0.13 (ALL-PIM-ROUTERS group). Routers do not send any acknowledgement that a Hello message was received. A hold time value determines the length of time for which the information is valid. In PIM-SM, a downstream receiver must join a group before traffic is forwarded on the interface.

- **Electing a Designated Router：** In a multi-access network with multiple routers connected, one of them is selected to act as a designated router (DR) for a given period of time. The DR is responsible for sending Join/Prune messages to the RP for local members.

- **Determining the RP：** PIM-SM uses a Bootstrap Router (BSR) to originate Bootstrap messages, and to disseminate RP information. The messages are multicast to the group on each link. If the BSR is not apparent, the routers flood the domain with advertisements. The router with the highest priority (if priorities are same, the higher IP address applies) is selected to be the RP. Routers receive and store Bootstrap messages originated by the BSR. When a DR gets a membership indication from IGMP for (or a data packet from) a directly connected host, for a group for which it has no entry, the DR maps the group address to one of the candidate RPs that can service that group. The DR then sends a Join/Prune message towards that RP. In a small domain, the RP can also be configured statically.

- **Joining the Shared Tree：** To join a multicast group, a host sends an IGMP message to its upstream router, after which the router can accept multicast traffic for that group. The router sends a Join message to its upstream PIM neighbor in the direction of the RP. When a router receives a Join message from a downstream router, it checks to see if a state exists for the group in its multicast routing table. If a state already exists, the Join message has reached the shared tree, and the interface from which the message was received is entered in the Outgoing Interface list. If no state exists, an entry is created, the interface is entered in the Outgoing Interface list, and the Join message is again sent towards the RP.

- **Registering with the RP：** A DR can begin receiving traffic from a source without having a Source or a Group state for that source. In this case, the DR has no information on how to get multicast traffic to the RP through a tree. When the source DR receives the initial multicast packet, it encapsulates it in a Register message, and unicasts it to the RP for that group. The RP decapsulates each Register message, and forwards the extracted data packet to downstream members on the RPT. Once the path is established from the source to the RP, the DR begins sending traffic to the RP as standard IP multicast packets, as well as encapsulated within Register messages. The RP temporarily receives packets twice. When the RP detects the normal multicast packets, it sends a Register-Stop message to the source DR, meaning it should stop sending register packets.

- **Sending Register-Stop Messages：** When the RP begins receiving traffic from the source, both as Register messages and as unencapsulated IP packets, it sends a Register-Stop message to the DR. This notifies the DR that the traffic is now being received as standard IP multicast packets on the SPT. When the DR receives this message, it stops encapsulating traffic in Register messages.

- **Pruning the Interface：** Routers attached to receivers send Prune messages to the RP to disassociate the source from the RP. When an RP receives a Prune message, it no longer forwards traffic from the source indicated in the Prune message. If all members of a multicast group are pruned, the IGMP state of the DR is deleted, and the interface is removed from the Source and Group lists of the group.

- **Forwarding Multicast Packets：** PIM-SM routers forward multicast traffic onto all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork, and have a Time to Live (TTL) of 1. The router performs an RPF check, and forwards the packet. Traffic that arrives on the correct interface is sent onto all outgoing interfaces that lead to downstream receivers if the downstream router has sent a join to this router, or is a member of this group.

5.2.2 Configuration

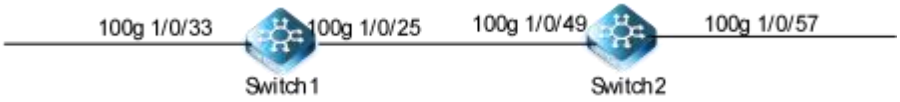


Figure 5-2 PIM-SM

PIM-SM is a soft-state protocol. The main requirement is to enable PIM-SM on desired interfaces, and configure the RP information correctly, through static or dynamic methods. All multicast group states are maintained dynamically as the result of IGMP Report/Leave and PIM Join/Prune messages.

This section provides PIM-SM configuration examples for two relevant scenarios. The following graphic displays the network topology used in these examples:

Configuring General PIM Sparse-mode (static RP)

In this example, using the above topology, Switch1 is the Rendezvous Point (RP), and all routers are statically configured with RP information. While configuring the RP, make sure that:

Every router includes the ip pim rp-address 11.1.1.1 statement, even if it does not have any source or group member attached to it.

There is only one RP address for a group scope in the PIM domain.

All interfaces running PIM-SM must have sparse-mode enabled.

Here is a sample configuration:

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode， set the attributes and ip address, and enable pim-sm

Configuring Switch 1.

```
switch1(config)#interface 10gigaethernet 1/0/33
switch1(config-10ge1/0/33)# port link-type trunk
switch1(config-10ge1/0/33)# no port trunk allow-pass vlan 1
switch1(config-10ge1/0/33)# port trunk allow-pass vlan 400
switch(config)#interface vlan 400
switch(config-vlanif-400)# ip address 20.1.20.1/24
switch(config-vlanif-400)# igmp enable
switch(config-vlanif-400)# ip pim-sm


switch(config)#interface 100gigaethernet 1/0/25
switch(config-100ge1/0/25)# port link-type trunk
switch(config-100ge1/0/25)# no port trunk allow-pass vlan 1
switch(config-100ge1/0/25)# port trunk allow-pass vlan 300
switch(config)#interface vlan 300
switch(config-vlanif-300)# ip address 20.1.23.2/24
switch(config-vlanif-300)# ip pim-sm

switch1(config)#interface loopback 1
switch1(config-loopback-1)# ip address 20.20.20.20/24
```

Configuring Switch 2.

```
switch2(config)#interface 100gigaethernet 1/0/49
switch2(config-100ge1/0/49)# port link-type trunk
switch2(config-100ge1/0/49)# no port trunk allow-pass vlan 1
switch2(config-100ge1/0/49)# port trunk allow-pass vlan 300
switch2(config)#interface vlan 300
switch2(config-vlanif-300)# ip address 20.1.23.3/24
switch2(config-vlanif-300)# ip pim-sm

switch2(config)#interface 10gigaethernet 1/0/57
switch2(config-10ge1/0/57)# port link-type trunk
```

```
switch2(config-10ge1/0/57)# no port trunk allow-pass vlan 1
switch2(config-10ge1/0/57)# port trunk allow-pass vlan 500
switch2(config)#interface vlan 500
switch2(config-vlanif-500)# ip address 20.1.30.1/24
switch2(config-vlanif-500)# igmp enable
switch2(config-vlanif-500)# ip pim-sm
```

step 3 Configure dynamic OSPF routes

Configuring Switch 1.

```
switch1(config)#router ospf 5
switch1(config-ospf-5)# router-id 20.1.20.1
  WARNING:Changing the parameter in this command resets the neighbor session.Continue?(y/n) [y]y
switch1(config-ospf-5)# network 20.1.20.1 255.255.255.255 area 0
switch1(config-ospf-5)# network 20.1.23.2 255.255.255.255 area 0
```

Configuring Switch 2.

```
switch2(config)#router ospf 5
switch2(config-ospf-5)# router-id 20.1.30.1
  WARNING:Changing the parameter in this command resets the neighbor session.Continue?(y/n) [y]y
switch2(config-ospf-5)# network 20.1.23.3 255.255.255.255 area 0
switch2(config-ospf-5)# network 20.1.30.1 255.255.255.255 area 0
switch1(config-ospf-5)#network 20.20.20.20 255.255.255.255 area 0
```

step 4 Configure the static rp address

```
switch1(config)#pim
switch1(config-pim)# rp-address 20.20.20.20 group default

switch2(config)#pim
switch2(config-pim)# rp-address 20.20.20.20 group default
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

Use the following command to display the mapping for the RP.RP is static configured for all multicast groups 224.0.0.0.0/4:

```
switch2(config)#show ip pim rp
  Group                RP                  Priority    State       BSR-Address          ExpiryTime(s)
Vpn-Instance: public net
  224.0.0.0/4          20.20.20.20         0           static      0.0.0.0              0
```

Use the following command to show the interface information:

```
switch1(config)#show ip pim config
!
ip multicast-routing
pim
 rp-address 20.20.20.20 group default
interface vlan200
 ip pim-sm
interface vlan300
 ip pim-sm
interface vlan400
 ip pim-sm
interface loopback1
 ip pim-sm

switch1(config)#show ip pim interface
  Interface                State   Nbr-Cnt    Hello-Interval    DR-Pri       DR-Address
  vlan200                  up      1          30                1            20.1.12.2
  vlan300                  up      1          30                1            20.1.23.3
  vlan400                  up      0          30                1            20.1.20.1
  loopback1                up      0          30                1            20.20.20.20

switch1(config)#show ip pim neighbor
  Neighbor-Address    Interface    DR prioruty    State        ExpiryTime(s)
  20.1.12.1           vlan200      1              NON-DR       86
  20.1.23.3           vlan300      1              DR           85
```

Use the following command to show the pim sparse-mode multicast routes:

Configuring Switch 1.

```
switch1(config)#show ip pim route
 Vpn-Instance: public net
 (*,225.0.0.1):  RP: 20.20.20.20
 Incoming Interface: N/A, RPF: N/A
 Outgoing Interface:
   vlan400          Forwarding    Expires: 00:00:00

 Vpn-Instance: public net
 (*,225.0.0.2):  RP: 20.20.20.20
 Incoming Interface: N/A, RPF: N/A
 Outgoing Interface:
vlan300          Forwarding    Expires: 00:03:21
```

Configuring Switch 2.

```
switch2(config)#show ip pim route
 Vpn-Instance: public net
 (*,225.0.0.2):  RP: 20.20.20.20
 Incoming Interface: vlan300, RPF: 20.1.23.2
 Outgoing Interface:
```

```
vlan500          Forwarding   Expires: 00:00:00
```

Configuring General PIM Sparse-mode (dynamic RP)

In a small and simple network, the multicast information is small, and the whole network can only rely on one RP for information forwarding. At this time, RP location can be statically specified on each router in the SM domain.However, in most cases, PIM-SM network has a large scale, and the multicast information forwarded by RP is huge. In order to relieve the burden of RP and optimize the topology structure of the Shared tree, different multicast groups should correspond to different RP. In this case, the bootstrapping mechanism is needed to dynamically elect RP.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode，set the attributes and ip address, and enable pim-sm

Configuring Switch 1.

```
switch1(config)#interface 10gigaethernet 1/0/33
switch1(config-10ge1/0/33)# port link-type trunk
switch1(config-10ge1/0/33)# no port trunk allow-pass vlan 1
switch1(config-10ge1/0/33)# port trunk allow-pass vlan 400
switch(config)#interface vlan 400
switch(config-vlanif-400)# ip address 20.1.20.1/24
switch(config-vlanif-400)# igmp enable
switch(config-vlanif-400)# ip pim-sm

switch(config)#interface 100gigaethernet 1/0/25
switch(config-100ge1/0/25)# port link-type trunk
switch(config-100ge1/0/25)# no port trunk allow-pass vlan 1
switch(config-100ge1/0/25)# port trunk allow-pass vlan 300
switch(config)#interface vlan 300
switch(config-vlanif-300)# ip address 20.1.23.2/24
switch(config-vlanif-300)# ip pim-sm

switch1(config)#interface loopback 1
switch1(config-loopback-1)# ip address 20.20.20.20/24
```

Configuring Switch 2.

```
switch2(config)#interface 100gigaethernet 1/0/49
switch2(config-100ge1/0/49)# port link-type trunk
switch2(config-100ge1/0/49)# no port trunk allow-pass vlan 1
switch2(config-100ge1/0/49)# port trunk allow-pass vlan 300
switch2(config)#interface vlan 300
switch2(config-vlanif-300)# ip address 20.1.23.3/24
switch2(config-vlanif-300)# ip pim-sm
switch2(config)#interface 10gigaethernet 1/0/57
```

```
switch2(config-10ge1/0/57)# port link-type trunk
switch2(config-10ge1/0/57)# no port trunk allow-pass vlan 1
switch2(config-10ge1/0/57)# port trunk allow-pass vlan 500
switch2(config)#interface vlan 500
switch2(config-vlanif-500)# ip address 20.1.30.1/24
switch2(config-vlanif-500)# igmp enable
switch2(config-vlanif-500)# ip pim-sm
```

step 3 Configure dynamic OSPF routes

Configuring Switch 1.

```
switch1(config)#router ospf 5
switch1(config-ospf-5)# router-id 20.1.20.1
  WARNING:Changing the parameter in this command resets the neighbor session.Continue?(y/n) [y]y
switch1(config-ospf-5)# network 20.1.20.1 255.255.255.255 area 0
switch1(config-ospf-5)# network 20.1.23.2 255.255.255.255 area 0
```

Configuring Switch 2.

```
switch2(config)#router ospf 5
switch2(config-ospf-5)# router-id 20.1.30.1
  WARNING:Changing the parameter in this command resets the neighbor session.Continue?(y/n) [y]y
switch2(config-ospf-5)# network 20.1.23.3 255.255.255.255 area 0
switch2(config-ospf-5)# network 20.1.30.1 255.255.255.255 area 0
```

step 4 Configure the candidate RP interface

Configuring Switch 1.

```
switch1(config)#interface loopback 1
switch1(config-loopback-1)# ip pim c-bsr group default
switch1(config-loopback-1)# ip pim c-rp group default
```

Configuring Switch 2.

```
switch2(config)#int vlan 300
switch2(config-vlanif-300)# ip pim c-bsr group default
switch2(config-vlanif-300)# ip pim c-rp group default
```

Note： The highest priority router is chosen as the RP. If two or more routers have the same priority, a hash function in the BSR mechanism is used to choose the RP, to make sure that all routers in the PIM-domain have the same RP for the same group.

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

Use the show ip pim sparse-mode rp mapping command to display the group-to-RP mapping details. The output displays information about RP candidates. There are two RP candidates for the group range 224.0.0.0/4. RP Candidate 20.20.20.20 has a default priority of 0, whereas, RP Candidate 20.1.23.3 has been configured to have a priority of 2. Since RP candidate 20.20.20.20 has a higher priority, it is selected as RP for the multicast group 224.0.0.0/24.

Configuring Switch 2.

```
switch2(config-vlanif-300)#show ip pim rp
 Group            RP              Priority   State     BSR-Address       ExpiryTime(s)
Vpn-Instance: public net
 224.0.0.0/4       20.1.23.3         2         no-static  20.20.20.20       97
224.0.0.0/4       20.20.20.20       0         no-static  20.20.20.20       97
```

To display information about the RP router for a particular group,use the following command.

Configuring Switch 2.

```
switch2(config)#show ip pim rp group 225.0.0.1
  Elected RP Address              :20.20.20.20
```

After RP information reaches all PIM routers in the domain, various state machines maintain all routing states as the result of Join/Prune from group membership. To display information on interface details and the multicast routing table, refer to the Configuring RP Statically section above.

Configuring IGMP SSM Mapping

Source-specific multicast (SSM) requires multicast routers to know which multicast sources hosts specify when they join a multicast group. A host running IGMPv3 can specify multicast source addresses in IGMPv3 Report messages. However, hosts running IGMPv1 or IGMPv2 rely on the IGMP SSM mapping function to obtain the SSM service.

IGMP SSM mapping is implemented based on static SSM mapping entries. A multicast router converts (*, G) information in IGMPv1 and IGMPv2 Report messages to (G, INCLUDE, (S1, S2...)) information according to static SSM mapping entries to provide the SSM service for IGMPv1 and IGMPv2 hosts.By default, the SSM group address range is 232.0.0.0 to 232.255.255.255.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enable SSM Mapping

Enable SSM Mapping function.

```
switch2(config)#interface vlan 500
switch2(config-vlanif-500)# igmp enable
switch2(config-vlanif-500)# igmp version v3
switch2(config-vlanif-500)# igmp ssm-mapping enable
```

Configure the group scope of the SSM Mapping application

```
switch2(config)# igmp
switch2(config-igmp)# igmp ssm-mapping filter-list 1500 source-address 20.1.20.2
```

step 3 Exit the configure mode

```
Switch(config-if)# end
```

step 4 Validation

```
switch2(config)#show igmp config
!
igmp start
igmp
 igmp ssm-mapping filter-list 1500 source-address 20.1.20.2

 Interface vlan500
 igmp enable
 igmp version v3
 igmp ssm-mapping enable

switch2(config)#show ip pim config
!
ip multicast-routing
pim
interface vlan300
 ip pim-sm
 ip pim c-bsr group default
 ip pim c-rp group 224.0.0.0/4 priority 2
interface vlan500
 ip pim-sm
```

5.2.3 Application cases

N/A

5.3 Configuring IGMP Snooping

5.3.1 Overview

Function Introduction

Internet Group Management Protocol Snooping (IGMP snooping) is a Layer 2 IPv4 multicast protocol. The IGMP snooping protocol maintains information about the outbound interfaces of multicast packets by snooping multicast protocol packets exchanged between the Layer 3 multicast device and user hosts. The IGMP snooping protocol manages and controls the forwarding of multicast packets at the data link layer.

Principle Description

IGMP Snooping can be enabled globally or per vlan. If IGMP Snooping is disabled globally, it can't be active on any vlan even it is enabled on the vlan. If IGMP snooping is enabled globally, it can be disabled on a vlan. On the other hand, the global configuration can overwrite the per vlan configuration. By default, IGMP snooping is enabled globally and per vlan.

The layer 2 switch controls the flooding of multicast traffic through IGMP Snooping.When the IGMP message transmitted between host and router is received by the layer 2 Ethernet exchange, the information contained in the IGMP message will be analyzed by IGMP Snooping, the port and MAC multicast address will be mapped, and the multicast data will be forwarded according to such mapping relationship.Multicast routers periodically send generic group queries to maintain multicast group membership.All recipients will respond to this query by sending an IGMP report packet, which is used by the switch to monitor the IGMP report packet to establish a forwarding entry.

Layer 2 multicast groups can be set up dynamically or statically through IGMP packets.A statically configured multicast group overrides a dynamically configured multicast group.

Limit and guide:

Multicast IP is used by protocols such as VRRP, RIP, OSPF, etc. Therefore, these 224.0.0.x multicast group addresses should be avoided in networks that enable IGMP Snooping to avoid collisions resulting in exceptions.

5.3.2 Configuration

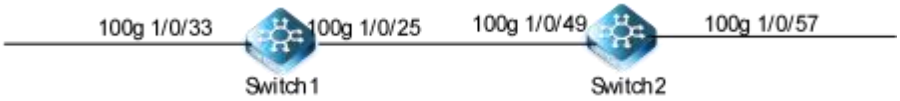


Figure 5-3 IGMP Snooping

Enable the IGMP Snooping

IGMP Snooping requires global and VLAN enablement.When IGMP Snooping is closed in global mode, it is not effective to enable IGMP Snooping only under the VLAN.When IGMP Snooping is turned on in global mode, you can optionally turn off IGMP Snooping under some VLANs.

step 1 Enter the configure mode

```
Switch#configure
```

step 2 Enable IGMP Snooping on global, VLAN, interface

```
Switch1(config)#igmp-snooping start
Switch1(config)#igmp-snooping mvlan 200
switch1(config)#interface 10gigaethernet 1/0/33
switch1(config-10ge1/0/33)#igmp-snooping enable
switch1(config-10ge1/0/33)#interface 100gigaethernet
1/0/25 switch1(config-100ge1/0/25)#igmp-snooping enable

switch2(config)#igmp-snooping start
switch2(config)#igmp-snooping mvlan 200
```

```
switch2(config)#interface 10gigaethernet 1/0/57
switch2(config-10ge1/0/57)#igmp-snooping enable
switch2(config-10ge1/0/57)#interface 100gigaethernet 1/0/49
switch2(config-100ge1/0/49)#igmp-snooping enable
switch2(config-100ge1/0/49)#
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

Use the following command to display igmp snooping.

```
switch2#show igmp-snooping   mvlan
MVLAN : 200
  Work Mode : snooping
  Version : v2
  Report Suppress : disable
  Leave Suppress : disable
  Forwarding mode : mac
  Max Response Time : 10
  Require Router Alert : disable
  Querier : disable
  802.1p Priority : default
  Proxy Ip : 0.0.0.0
  Multicast Vlan : disable
  SSM Mapping : disable
  Lastmember Query Interval : 1
  Lastmember Query Number : 2
  Proxy Uplink Port : disable
  Uplink Port Limit : 1
  Uplink Port Drop Report : enable
  Fast Switch : enable
  Fast Switch Query : enable
  Query Srouce Ip : 192.168.0.1
```

Configuring Fast Leave

When IGMP Snooping fast leave is enabled, the igmp snooping group will be removed at once upon receiving a corresponding igmp report. Otherwise the switch will send out specified igmp specific query, if it doesn't get response in specified period, it will remove the group. By default, igmp snooping fast-leave is disabled globally and per vlan.

step 1 Enter the configure mode

```
Switch#configure
```

step 2 Enable Fast Leave

```
Switch(config)#ip igmp snooping fast-leave
Switch(config)#ip igmp snooping vlan 1 fast-leave
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

```
switch2#show igmp-snooping interface
  Interface          State      Ctrlmode   Fastleave Grouplimit   Drop     Action   GroupPolicy
  100ge1/0/49        enable     disable    disable   1000         ---      delay    ---
  10ge1/0/57         enable     disable    enable    1000         ---      delay    ---
```

Configuring Query Parameters

In order for IGMP, and thus IGMP snooping, to function, an multicast router must exist on the network and generate IGMP queries. The tables created for snooping (holding the member ports for a each multicast group) are associated with the querier. Without a querier the tables are not created and snooping will not work.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Set the global attributes of igmp snooping

```
switch1(config)#igmp-snooping query-interval 50
switch1(config)#igmp-snooping robust-count 3
switch1(config)#igmp-snooping lastmember-queryinterval 2
switch1(config)#igmp-snooping max-response-time 5
```

step 3 Set the vlan attributes of igmp snooping

```
switch1(config)#igmp-snooping mvlan 200
switch1(config-igmpsnoop-mvlan200)# igmp-snooping querier enable
switch1(config-igmpsnoop-mvlan200)# igmp-snooping lastmember-queryinterval 1
switch1(config-igmpsnoop-mvlan200)# igmp-snooping lastmember-querynumber 3
switch1(config-igmpsnoop-mvlan200)# igmp-snooping send-query source-address 20.1.20.5
switch1(config-igmpsnoop-mvlan200)# igmp-snooping max-response-time 5
```

step 4 Exit the configure mode

```
Switch(config)# end
```

step 5 Validation

```
switch1(config)#show igmp-snooping config
!
igmp-snooping start
igmp-snooping robust-count 3
igmp-snooping query-interval 50
igmp-snooping max-response-time 5
igmp-snooping lastmember-queryinterval 2
igmp-snooping mvlan 200
 igmp-snooping forwarding-mode ip
 igmp-snooping version v3
 igmp-snooping max-response-time 5
 igmp-snooping querier enable
 igmp-snooping lastmember-queryinterval 1
 igmp-snooping lastmember-querynumber 3
 igmp-snooping send-query source-address 20.1.20.5

switch1(config)#show igmp-snooping
  Version                        :IGMPSNOOP_VB3.03.00.00
  Igmp-snooping                   : start
  Robustness                      : 3
  Query Interval                 : 50 seconds
  Max Response Time               : 5 seconds
  Lastmember Query Interval      : 2 seconds
  V2router Aging Time             : 180 seconds

switch1(config)#show igmp-snooping mvlan
MVLAN : 200
  Work Mode : snooping
  Version : v3
  Report Suppress : disable
  Leave Suppress : disable
  Forwarding mode : ip
  Max Response Time : 5
  Require Router Alert : disable
  Querier : enable
  802.1p Priority : default
  Proxy Ip : 0.0.0.0
  Multicast Vlan : disable
  SSM Mapping : disable
  Lastmember Query Interval : 1
  Lastmember Query Number : 3
  Proxy Uplink Port : disable
  Uplink Port Limit : 1
  Uplink Port Drop Report : enable
  Fast Switch : enable
```

```
Fast Switch Query : enable
Query Srouce Ip : 20.1.20.5
```

Configure the IGMP Snooping multicast routing port

A multicast routing port is a port on a switch that is connected to a multicast router and can be dynamically learned or statically configured.When an IGMP generic group query packet or PIMv2 Hello packet is received on a VLAN port, the port becomes the multicast routing port of the VLAN.All IGMP query packets received from the multicast routing port are broadcast within the VLAN to which they belong.IGMP report/leave packets received on all VLANs will also be forwarded from the multicast routing port (in the case of packet suppression shutdown), and all multicast traffic received on that VLAN will be forwarded from the multicast routing port.

step 1 Enter the configure mode

```
Switch#configure
```

step 2 Configure static multicast routing ports

```
switch1(config)# igmp-snooping mvlan 200
switch1(config-igmpsnoop-mvlan200)#igmp-snooping uplink-port 10gigaethernet 1/0/33
```

step 3 Validation

```
switch1(config)#show igmp-snooping   uplinkport
  Mvlan    UplinkPort       Expires          Type
  200      10ge1/0/33       ---              static
```

Configure STP ring topology changes for quick switching

When the topology of the two-layer network changes, the forwarding path of the group broadcast may change.When the router is configured to actively send IGMP Query message in case of link failure, when the member of the multicast group responds to the IGMP Report message, the device updates the member port information according to the Report message and switches the multicast data stream to the new forwarding path in time.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enable the ability to send IGMP universal group query packets when the device network topology changes

```
switch1(config)# igmp-snooping mvlan 200
switch1(config-igmpsnoop-mvlan200)#igmp-snooping fast-switch enable
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

```
switch1(config)#show igmp-snooping mvlan
MVLAN : 200
  Work Mode : snooping
  Version : v2
  Report Suppress : disable
  Leave Suppress : disable
  Forwarding mode : mac
  Max Response Time : 10
  Require Router Alert : disable
  Querier : enable
  802.1p Priority : default
  Proxy Ip : 0.0.0.0
  Multicast Vlan : disable
  SSM Mapping : disable
  Lastmember Query Interval : 1
  Lastmember Query Number : 2
  Proxy Uplink Port : disable
  Uplink Port Limit : 1
  Uplink Port Drop Report : enable
  Fast Switch : enable
  Fast Switch Query : enable
  Query Srouce Ip : 20.1.20.5
```

Configure the IGMP Snooping Proxy

When a three-tier device is not IGMP enabled, such as when only a static multicast group is configured, there is no IGMP query in the network to maintain group membership.The IGMP Snooping Proxy function can be configured on the layer 2 device to send Query packets to act as IGMP queriers.When IGMP is running in the network, in order to reduce the number of IGMP Report packets and Leave packets received by the upstream three-tier devices, the IGMP Snooping Proxy function can be deployed on the second-tier devices to enable them to Proxy the downstream hosts to send membership Report packets to the upstream devices.A device configured with IGMP Snooping Proxy function is called the IGMP Snooping Proxy, which, in the view of its upstream device, is equivalent to a host.In the view of its downstream devices, it is equivalent to a query.

step 1 Enter the configure mode

```
Switch#configure
```

step 2 Enable the IGMP-Snooping Proxy

```
switch1(config)# igmp-snooping mvlan 200
switch1(config-igmpsnoop-mvlan200)#  igmp-snooping forwarding-mode ip
switch1(config-igmpsnoop-mvlan200)#  igmp-snooping workmode igmp-proxy
switch1(config-igmpsnoop-mvlan200)#  igmp-snooping version v3
switch1(config-igmpsnoop-mvlan200)#  igmp-snooping proxy-ip 20.1.20.5
switch1(config-igmpsnoop-mvlan200)#  igmp-snooping querier enable
```

```
switch1(config-igmpsnoop-mvlan200)#   igmp-snooping proxy-uplink-port enable
switch1(config-igmpsnoop-mvlan200)#igmp-snooping uplink-port 10gigaethernet 1/0/33
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

```
switch1(config)#show igmp-snooping config
!
igmp-snooping start
igmp-snooping mvlan 200
 igmp-snooping forwarding-mode ip
 igmp-snooping workmode igmp-proxy
 igmp-snooping version v3
 igmp-snooping proxy-ip 20.1.20.5
 igmp-snooping querier enable
 igmp-snooping uplink-port 10gigaethernet 1/0/33
 igmp-snooping proxy-uplink-port enable

switch1(config)#show igmp-snooping mvlan
MVLAN : 200
  Work Mode : proxy
  Version : v3
  Report Suppress : disable
  Leave Suppress : disable
  Forwarding mode : ip
  Max Response Time : 10
  Require Router Alert : disable
  Querier : enable
  802.1p Priority : default
  Proxy Ip : 20.1.20.5
  Multicast Vlan : disable
  SSM Mapping : disable
  Lastmember Query Interval : 1
  Lastmember Query Number : 2
  Proxy Uplink Port : enable
  Uplink Port Limit : 1
  Uplink Port Drop Report : enable
  Fast Switch : enable
  Fast Switch Query : enable
  Query Srouce Ip : 192.168.0.1
```

Configuring IGMP-Snooping Static group

An IGMP Snooping group record is created when the switch receives an IGMP message on the layer 2 port.At present, the system also supports static configuration of group records of IGMP Snoopoing. In the static configuration, group address, two-layer port, and VLAN belonging to the two-layer port should be specified.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure static group

```
switch2(config)#interface 10gigaethernet 1/0/57
switch2(config-10ge1/0/57)# igmp-snooping static-group group-address 225.0.0.1 mvlan 200
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

```
switch2(config)#show igmp-snooping group
  Total Entry(s) : 1
  Group Address     MVlan    Pre-join    MemNum   V3FilterMode
  225.0.0.1         200      disable     1        invalid

switch2(config)#show igmp-snooping egress-port
Total Entry(s) : 1

Group Address : 225.0.0.1
MVlan : 200
Source Address : *
Interface : 10ge1/0/57
    Type : static
    Expires : ---
    Out Vlan : 200
    V3 Mode : invalid

switch2(config)#show igmp-snooping source-address
Total Entry(s) : 1
MVlan Source Address   Group Address     Mode
200   *                225.0.0.1         exclude
```

5.3.3 Application cases

N/A

6 Security Configuration Guide

6.1 Configuring ACL

6.1.1 Overview

Function Introduction

ACL (Access Control List) is mainly used to realize flow identification, Access Control functions.In order to filter packets, network devices need to configure a series of matching rules to identify the packets to be filtered.Only after a particular packet has been identified can the packet be allowed to pass through according to the predefined policy.Acls categorize packets by a series of matching criteria, such as source address, destination address, port number, and so on.

Principle Description

The following terms and concepts are used to describe ACL：

- **Access control entry (ACE):** Each ACE includes an action element (permit or deny) and a series of filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.
- **MAC ACL:** MAC ACL can filter packet by mac-sa and mac-da, and the mac-address can be masked, or configured as host id, or configured as any to filter all MAC addresses. MAC ACL can also filter other L2 fields such as COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, L2 type, L3 type.
- **IPv4 ACL:** IPv4 ACL can filter packet by ip-sa and ip-da, and ip-address can be masked, or configured as host id, or configured as any to filter all IPv4 address. IPv4 ACL can also filter other L3 fields such as DSCP, L4 protocol and L4 fields such as TCP port, UDP port, and so on.
- **Time Range:** Time range can define a period of time only between which the ACE can be valid if the ACE is associated to the time range.

6.1.2 Configuration

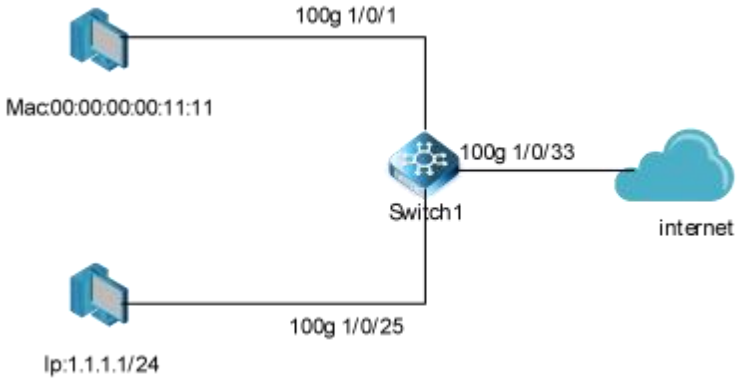


Figure 6-1 ACL

In this example, use MAC ACL on interface 100g 1/0/1, to permit packets with source mac 0000.0000.1111 and deny any other packets. Use IPv4 ACL on interface 100g 1/0/25, to permit packets with source ip 1.1.1.1/24 and deny any other packets.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Create access list

L2 Access Control List:

```
switch1(config)# filter-list 100 name l2
switch1(configure-filter-l2-100)# filter 5 mac 00:00:00:00:11:11/48 any
switch1(configure-filter-l2-100)# filter 5 action permit
switch1(configure-filter-l2-100)# filter 100 mac any any
switch1(configure-filter-l2-100)# filter 100 action deny
```

L3 Access Control List:

```
switch1(config)# filter-list 1500 name l3
switch1(configure-filter-ipv4-1500)# filter 5 ip 1.1.1.1/32 any
switch1(configure-filter-ipv4-1500)# filter 5 action permit
switch1(configure-filter-ipv4-1500)#
switch1(configure-filter-ipv4-1500)# filter 100 ip any any
switch1(configure-filter-ipv4-1500)# filter 100 action deny
```

step 3 Apply the policy on the interface

```
switch1(config)#int 100g 1/0/1
switch1(config-100ge1/0/1)#filter-list in 100
switch1(config-100ge1/0/1)#exit

switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#filter-list in 1500
```

step 4 Exit the configure mode

```
Switch(config)# end
```

step 5 Validation

The result of show running-config is as follows:

```
switch1(config)#show filter-list config

 filter-list 100 name l2 filter 2
 filter-list 100 name l2
 filter 5 mac 00:00:00:00:11:11/48 any
 filter 5 action permit

 filter 100 mac any any
```

```
filter 100 action deny

filter-list 1500 name l3 filter 2
filter-list 1500 name l3
filter 5 ip 1.1.1.1/32 any
filter 5 action permit

filter 100 ip any any
filter 100 action deny

interface 100ge1/0/1
filter-list in name l2

interface 100ge1/0/25
filter-list in name l3
```

6.1.3 Application cases

N/A

6.2 Configuring Extern ACL

6.2.1 Overview

Function Introduction

Extend IPv4 ACL combines MAC filters with IP filters in one access list. Different from MAC and IP ACL, extend ACL can access-control all packets (IP packets and non-IP packets). Extend ACL supported extend IPv4 ACL.

Principle Description

Following is a brief description of terms and concepts used to describe the extend ACL：

- **Extend IPv4 ACL：** Extend IPv4 ACL takes advantages of MAC ACL and IPv4 ACL, which combines MAC ACE with IPv4 ACE in an ACL to provide more powerful function of access-controlling traverse packets.
- **MAC ACE：** Filter packets by mac-sa and mac-da, and the mac-address can be masked, or configured as host id, or configured as any to filter all MAC addresses. Other L2 fields, such as COS, VLAN-ID, INNER-COS, INNER-VLAN-ID, L2 type, L3 type, can also be filtered by MAC ACE.
- **IPv4 ACE：** Filter packets by ip-sa and ip-da, and ip-address can be masked, or configured as host id, or configured as any to filter all IPv4 address. Other L3 fields such as DSCP, L4 protocol and L4 fields, such as TCP port, UDP port, can also be filtered by IPv4 ACE.

The MAC ACE and IPv4 ACE in an extend IPv4 ACL can be configured alternately in arbitrary order which is completely specified by user.

6.2.2 Configuration

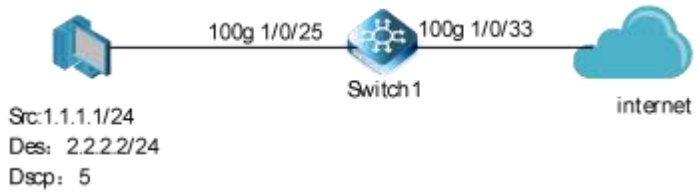


Figure 6-2 extern acl

In this example, use extend IPv4 ACL on interface eth-0-1, to permit packets with source mac 0000.0000.1111 and cos value of 2, permit all TCP packets, and deny any other packets.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Create access list

```
switch1(config)# filter-list 1500 name l3
switch1(configure-filter-ipv4-1500)# filter 5 ip 1.1.1.1/32 2.2.2.2/32 dscp cs5
switch1(configure-filter-ipv4-1500)# filter 5 action permit
switch1(configure-filter-ipv4-1500)#
switch1(configure-filter-ipv4-1500)# filter 10 tcp any any any any
switch1(configure-filter-ipv4-1500)# filter 10 action permit
switch1(configure-filter-ipv4-1500)#
switch1(configure-filter-ipv4-1500)# filter 100 ip any any
switch1(configure-filter-ipv4-1500)# filter 100 action deny
```

step 3 Apply the policy on the interface

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#filter-list in 1500
```

step 4 Exit the configure mode

```
Switch(config)# end
```

step 5 Validation

The result of show running-config is as follows:

```
switch1#show filter-list config
filter-list 1500 name l3 filter 3
filter-list 1500 name l3
filter 5 ip 1.1.1.1/32 2.2.2.2/32 dscp cs5
filter 5 action permit
```

```
filter 10 tcp any any any any
filter 10 action permit

interface 100ge1/0/25
filter-list in name l3

switch1#show filter-list interface
Filter-list Interface          Dir Name
  1500              100ge1/0/25       In   l3
```

6.2.3 Application cases

N/A

6.3 Configuring IPv6 ACL

6.3.1 Overview

Function Introduction

Access control lists for IPv6 (ACLv6) classify traffic with the same characteristics. The ACLv6 can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet. ACLv6 can filter packets received on interface by many fields such as ipv6 address and deny or permit the packets.

Principle Description

The following terms and concepts are used to describe ACLv6.

- **Access control entry (ACE)：** Each ACE includes an action element (permit or deny) and a filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.
- **IPv6 ACL：** IPv6 ACL can filter packet by ipv6-sa and ipv6-da, and ipv6-address can be masked, or configured as host id, or configured as any to filter all IPv6 address. IPv6 ACL can also filter other L3 fields such as L4 protocol and L4 fields such as TCP port, UDP port, and so on.
- **Time Range：** Time range can define a period of time only between which the ACE can be valid if the ACE is associated to the time range.

6.3.2 Configuration

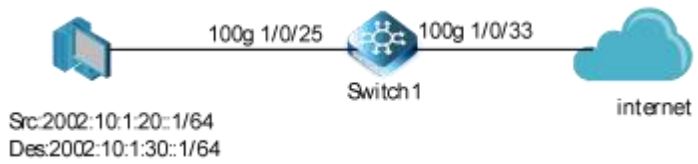


Figure 6-3 ipv6 acl

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Create access list

ipv6 access list:

```
switch1(config)# filter-list 3100 name ipv6
switch1(configure-filter-ipv6-3100)# filter 5 ip6 2002:10:1:20::1/64 2002:10:1:30::1/64
switch1(configure-filter-ipv6-3100)# filter 5 action permit
switch1(configure-filter-ipv6-3100)#
switch1(configure-filter-ipv6-3100)# filter 10 tcp6 any any any any
switch1(configure-filter-ipv6-3100)# filter 10 action permit
switch1(configure-filter-ipv6-3100)#
switch1(configure-filter-ipv6-3100)# filter 100 ip6 any any
switch1(configure-filter-ipv6-3100)# filter 100 action deny
```

step 3 Apply the policy to the interface

```
switch1(config)#interface 100gigaethernet 1/0/25
switch1(config-100ge1/0/25)#filter-list in 3100
```

step 4 Exit the configure mode

```
Switch1(config)# end
```

step 5 Validation

```
switch1(config)#show running-config
filter-list 3100 name ipv6 filter 3
 filter-list 3100 name ipv6
 filter 5 ip6 2002:10:1:20::1/64 2002:10:1:30::1/64
 filter 5 action permit

 filter 10 tcp6 any any any any
 filter 10 action permit

 filter 100 ip6 any any
 filter 100 action deny

interface 100ge1/0/25
 filter-list in name ipv6

switch1#show filter-list interface
  Filter-list Interface          Dir Name
  100         100ge1/0/1         In  l2
  3100        100ge1/0/25        In  ipv6
```

6.3.3 Application cases

N/A

6.4 Configuring AAA

6.4.1 RADIUS Overview

Function Introduction

Authentication verifies users before they are allowed access to the network and network services. System can use AAA authentication methods and Non-AAA authentication methods. RADIUS Authentication is one of AAA authentication methods.

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS is widely used protocol in network environments. It is commonly used for embedded network devices such as routers, modem servers, switches, etc. RADIUS clients run on support routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

Principle Description

N/A

6.4.2 RADIUS Configuration

Figure 6-4 Private Vlan

The figure above is the networking topology for RADIUS authentication functions. We need one Switch and two computers for this test.

One computer as RADIUS server and configure the network card address 20.1.12.2/24.

Switch has RADIUS authentication function. The 25G 1/0/10 interface with Switch is added with VLAN 100, and the IP address is 20.1.12.1/24.The IP address of Switch management port is 10.32.133.115, and the IP address of PC connected to Switch management port is 172.100.10.103.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enable AAA and Radius server

```
switch(config)#aaa
switch(config-aaa)#radius-server hello ip-address 172.100.10.103 key 123456
switch(config-aaa)# server-group test1 radius-server hello
switch(config-aaa)# aaa authentication login method radius server-group test1
switch(config-aaa)#exit
```

step 3 Configure layer 3 interface IP addresses

```
switch(config)#interface 100gigaethernet 1/0/10
```

```
switch(config-100ge1/0/10)# port link-type access
switch(config-100ge1/0/10)# port default vlan 100
switch(config-100ge1/0/10)#exit
switch(config)#interface vlan 100
switch(config-vlanif-100)# ip address 20.1.12.1 255.255.255.0
```

step 4 configure authentication mode

```
switch(config)# line vty 1
switch(config-line)# login authentication aaa method radius auth-type pap
```

step 5 Exit the configure mode

```
Switch(config-line)# end
```

step 6 Validation

You can use command show authentication status in switch:

```
switch#show aaa server
Server Name                          : hello
  Server IP Address                  : 172.100.10.103
  Server IP Instance                 : public
  Server Source IP Instance          : public
  Server Key                         : $9$kijv$e7015e4ca31c3ae8bb69fcd561d01a6d
  Server Protocol Type               : radius
  Radius-server Authentication Port  : 1812
  Radius-server Accounting Port      : 1813
  Radius-server Retransmit Interval  : 2
  Radius-server Max Retransmit       : 3
  Radius-server Deadtime             : 60
  Radius-server Source IP Address    : N/A
  Server State                       : active
```

You can use command show keys in switch:

```
switch3#show aaa method
Method Name                          : radius
  Method Apply Type                  : login
  Method Apply Funtion               : authentication
  Method Local                       : disable
  Method None                        : disable
  Method Group List                  : test1
```

Telnet test is carried out. If the Telnet connection is configured correctly, the result information is similar to the following figure:

Figure 6-5 Telnet connecting test

Note： Don't forget to turn RADIUS authentication feature on.Make sure the cables is linked correctly You can use command to check log messages if Switch can't do RADIUS authentication:

```
switch#show logbuffer
```

6.4.3 RADIUS Application cases

N/A

Radius server configuration (Using WinRadius for example)

Set ip address for PC :

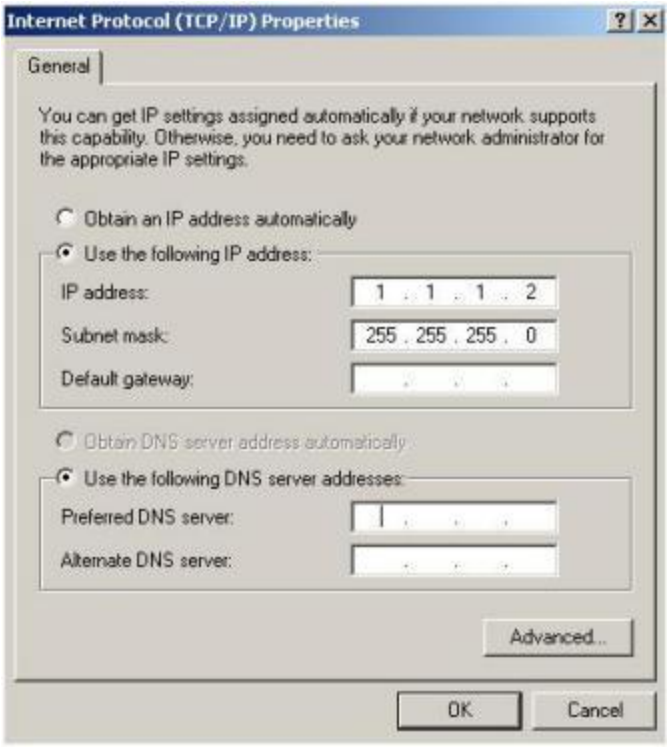


Figure 6-6 Set IP address for PC

Connectivity test between server and switch :

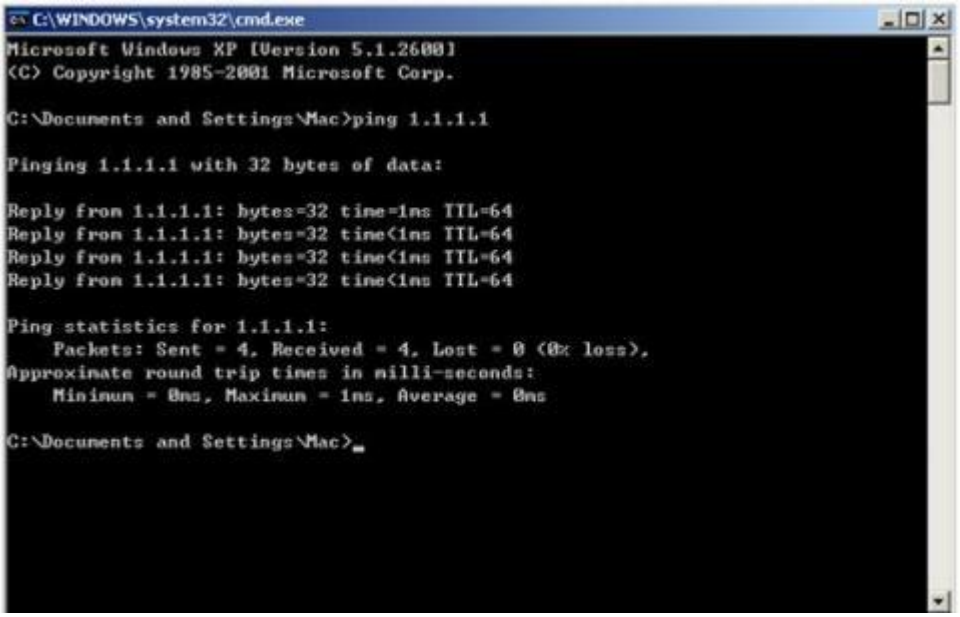


Figure 6-7 Connectivity test

Open winRadius:

Figure 6-8 WinRadius

Configurations for winRadius:

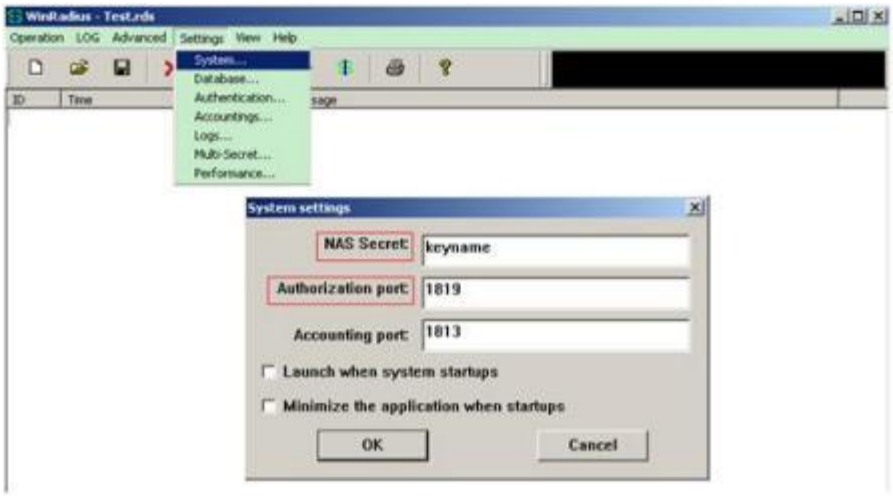


Figure 6-9 WinRadius

Add user and password :

Figure 6-10 Add user and password

Connectivity test between client and switch:

```
C:\Documents and Settings\mac>ping 10.10.29.215

Pinging 10.10.29.215 with 32 bytes of data:

Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.29.215:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 6-11 Connectivity test

6.4.4 TACACS+ Overview

Function Introduction

Authentication verifies users before they are allowed access to the network and network services. System can use AAA authentication methods and Non-AAA authentication methods. TACACS+ Authentication is one of AAA authentication methods.

TACACS+ is a distributed client/server system that secures networks against unauthorized access. TACACS+ is widely used protocol in network environments. It is commonly used for embedded network devices such as routers, modem servers, switches, etc. TACACS+ clients run on support routers and switches. Clients send authentication requests to a central TACACS+ server, which contains all user authentication and network service access information.

Principle Description

N/A

6.4.5 TACACS+ Configuration

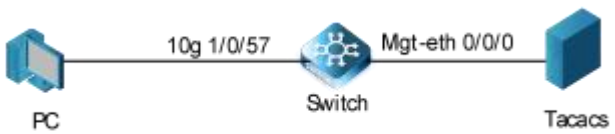


Figure 6-12 TACACS+

The figure above is the networking topology for TACACS+ authentication functions. We need one Switch and two computers for this test. One computer as TACACS+ server, it ip address of the eth0 interface is 1.1.1.2/24. Switch has TACACS+ authentication function. The ip address of interface eth-0-23 is 1.1.1.1/24. The management ip address of switch is 10.10.29.215, management port (only in-band management port) is connected the PC for test login, PC's ip address is 10.10.29.10

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enable AAA and TACACS + server

```
switch(config)#aaa
switch(config-aaa)# tacacs-server hello2 ip-address 172.100.10.103 key 123456
switch(config-aaa)# server-group test2 tacacs-server hello2
switch(config-aaa)# aaa authentication login method tacacs server-group test2
```

step 3 Configure a layer 3 interface and set ip address

```
switch(config)#interface 100gigaethernet 1/0/10
switch(config-100ge1/0/10)# port link-type access
switch(config-100ge1/0/10)# port default vlan 100
switch(config-100ge1/0/10)#exit
switch(config)#interface vlan 100
switch(config-vlanif-100)# ip address 20.1.12.1 255.255.255.0
```

step 4 Configure authentication mode

```
switch(config)#line vty 1
switch(config-line)# login authentication aaa method tacacs auth-type pap
```

step 5 Exit the configure mode

```
Switch(config-line)# end
```

step 6 Validation

Use the Show Authentication Status command to check the configuration

```
switch3(config)#show aaa server
Server Name                          : hello2
  Server IP Address                  : 172.100.10.103
  Server IP Instance                 : public
  Server Source IP Instance          : public
  Server Key                         : $9$kijv$e7015e4ca31c3ae8bb69fcd561d01a6d
  Server Protocol Type               : tacacs
  Tacacs-server Port                 : 49
  Tacacs-server Timeout              : 2
  Tacacs-server Deadtime             : 60
  Tacacs-server Single Connection    : disable
  Tacacs-server Source IP Address    : N/A
  Server State                       : active
```

Use the show aaa method-lists authentication command to check the AAA

```
switch3(config)#show aaa method
Method Name                    : tacacs
  Method Apply Type            : login
  Method Apply Funtion         : authentication
  Method Local                 : disable
  Method None                  : disable
  Method Group List            : test2
```

Telnet test is carried out. If the Telnet connection is configured correctly, the result information is similar to the following figure:

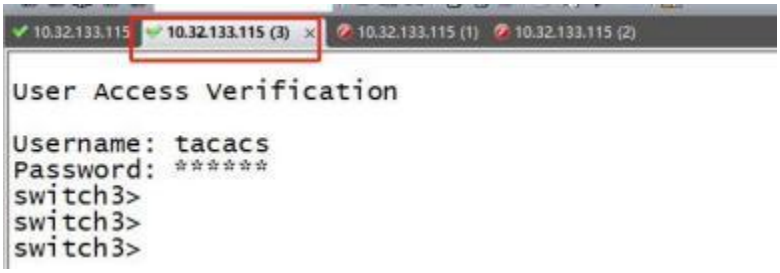


Figure 6-13 Telnet connecting test+

6.4.6 TACACS+ Application cases

Radius server configuration

step 1 Install the ACS server.

step 2 Configure the client interface on tacacs server.

Figure 6-14 tacas server

step 3 Configure the server configuration on the Tacacs server

Figure 6-15 tacas server

Figure 6-16 tacas server

step 4 Configure the Tacacs user

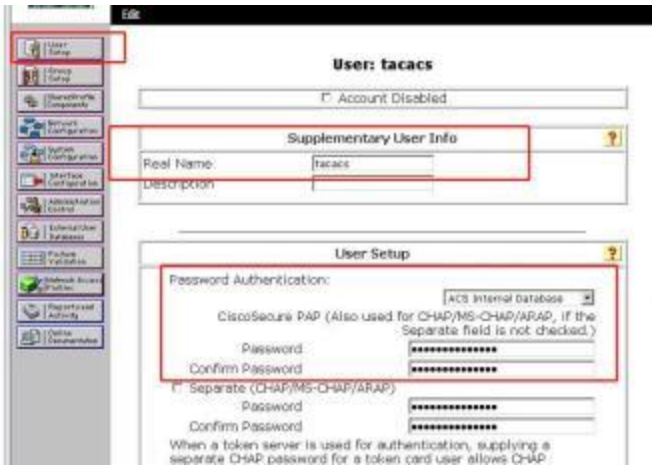


Figure 6-17 Configure the Tacacs user

step 5 Configure tacacs users to join groups

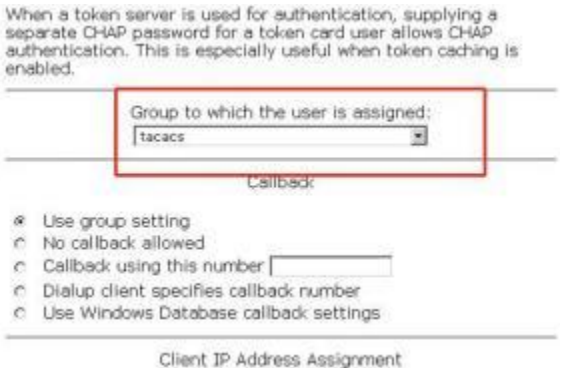


Figure 6-18 Configure tacacs users to join groups

step 6 Tacacs authentication

Figure 6-19 Tacacs certification

6.5 Configuring DHCP Snooping

6.5.1 Overview

Function Introduction

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers.

The DHCP snooping feature performs the following activities:

- **Validate DHCP messages received from untrusted sources and filters out invalid messages.**
- **Build and maintain the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.**
- **Utilize the DHCP snooping binding database to validate subsequent requests from untrusted hosts.**

Other security features, such as dynamic ARP inspection (DAI), also use information stored in the DHCP snooping binding database. DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs. The DHCP snooping feature is implemented in software basis. All DHCP messages are intercepted in the BAY and directed to the CPU for processing.

Principle Description

N/A

6.5.2 Configuration

Figure 6-20 DHCP Snooping

This figure is the networking topology for testing DHCP snooping functions.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure ports to allow the specified VLAN

```
switch (config)#vlan 1000
switch(config-100ge1/0/27)#port hybrid vlan 1000 tagged
switch(config-100ge1/0/27)#int 100g 1/0/31
switch(config-100ge1/0/31)#port hybrid  vlan 1000 tagged
switch(config-100ge1/0/31)#quit
switch(config)#int 100g 1/0/27
switch(config-100ge1/0/27)#port hybrid  vlan 1000 tagged
switch(config-100ge1/0/27)#quit
```

step 3 Configure the DHCP Snooping

```
switch(config)#dhcp-snooping start
switch(config)#vlan 1000
switch(vlan-1000)#dhcp-snooping enable
switch(vlan-1000)#dhcp-snooping  trust interface 100g 1/0/31
switch(vlan-1000)#quit
```

step 4 Exit the configure mode

```
Switch(config)# exit
```

step 5 Validation

Check the interface configuration.

```
switch (config)#show running-config
!
dhcp-snooping start
!
vlan 1000
 dhcp-snooping enable
 dhcp-snooping trust interface 100gigaethernet 1/0/31
```

Check the DHCP Snooping configuration.

```
switch(config)#show dhcp-snooping config
 Version:DHCPSNOOP_VB3.00.03.00
!
dhcp-snooping start
vlan 1000
 dhcp-snooping enable
 dhcp-snooping trust interface 100gigaethernet 1/0/31
```

```
switch(config)#
```

Check the dhcp snooping statistics.

```
switch(config)#show dhcp-snooping statistic
Interface : vlan1000
 Source mac mismatch : 0
 Binding entry mismatch : 0
 Untrust reply received : 0
```

Check the dhcp snooping binding information.

```
switch(config)#show dhcp-snooping binding

Total Number:1
IP-Addr          Mac-Addr           Vlan Interface      Time    AgeTime   State
100.1.1.5        68:21:5f:b7:5b:10  1000 100ge1/0/27    180     43        dynamic
```

6.5.3 Application cases

N/A

6.6 Configuring IP source guard

6.6.1 Overview

Function Introduction

IP source guard prevents IP spoofing by allowing only the IP addresses that are obtained through DHCP snooping on a particular port. Initially, all IP traffic on the port is blocked except for the DHCP packets that are captured by DHCP snooping. When a client receives a valid IP address from the DHCP server, an access control list (ACL) is installed on the port that permits the traffic from the IP address. This process restricts the client IP traffic to those source IP addresses that are obtained from the DHCP server; any IP traffic with a source IP address other than that in the ACL's permit list is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address.

IP source guard uses source IP address filtering, which filters the IP traffic that is based on its source IP address. Only the IP traffic with a source IP address that matches the IP source binding entry is permitted. A port's IP source address filter is changed when a new DHCP-snooping binding entry for a port is created or deleted. The port ACL is modified and reapplied in the hardware to reflect the IP source binding change. By default, if you enable IP source guard without any DHCP-snooping bindings on the port, a default ACL that denies all IP traffic is installed on the port. When you disable IP source guard, any IP source filter ACL is removed from the port.

Also IP source guard can use source IP and MAC address Filtering. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP and Mac addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table. If not, the switch drops all other types of packets except DHCP packet.

The switch also supports to have IP, MAC and VLAN Filtering. When IP source guard is enabled with this option, IP traffic is filtered cased on the source IP and MAC addresses. The switch forwards traffic only when the source IP, MAC addresses and VLAN match an entry in the IP source binding table.

Principle Description

The following terms and concepts are used to describe the IP source guard:

- **Dynamic Host Configuration Protocol (DHCP) :** Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

- **DHCP Snooping :** DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. This feature builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.

- **ACL :** Access control list.

6.6.2 Configuration

Configure ip source guard

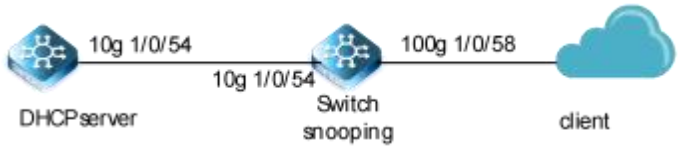


Figure 6-21 IP source guard

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the vlan configure mode and create vlan

```
switch(config)#int 100g 1/0/54
switch(config-100ge1/0/54)#port link-type access
switch(config-100ge1/0/54)#port default vlan 1000
switch(config)#quit
switch(config)#int 10g 1/0/58
switch(config-10ge1/0/58)#port link-type access
switch(config-10ge1/0/58)#port default vlan 1000
switch(config-10ge1/0/58)#quit
```

step 3 Configure DHCP Snooping

```
switch(config)#vlan 1000
switch(vlan-1000)#dhcp-snooping enable
switch(vlan-1000)#dhcp-snooping trust interface 100gigaethernet 1/0/54
```

step 4 Enables IP source guard (Default is based on IP + MAC + VLAN)

```
switch(config)#int 10g 1/0/58
switch(config-10ge1/0/58)#ip source check user-bind enable
switch(config-10ge1/0/58)#quit
```

step 5 Exit the configure mode

```
Switch(config)# exit
```

step 6 Validation

```
switch(config)#show ip source check user-bind

 interface 10gigaethernet 1/0/58
 ip source check user-bind enable
 ip source check dropped IP packets 0/0
```

6.6.3 Application cases

N/A

6.7 Configuring Private-vlan

6.7.1 Overview

Function Introduction

Private-vlan a security feature which is used to prevent from direct l2 communication among a set of ports in a vlan.

It can provide a safer and more flexible network solutions by isolating the ports which in the same VLAN.

Principle Description

N/A

6.7.2 Configuration

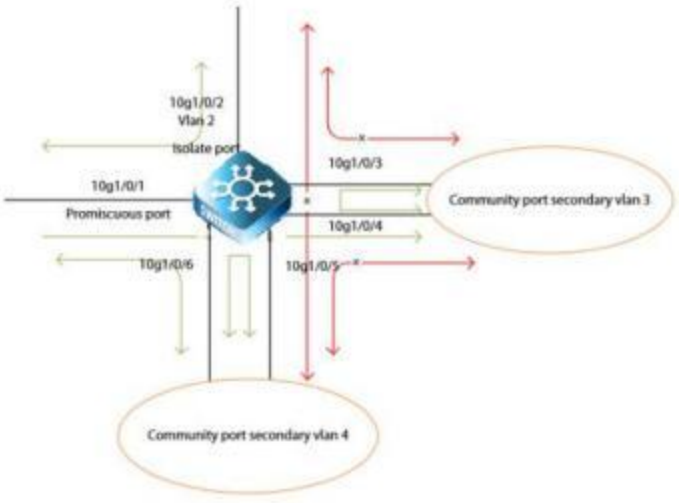


Figure 6-22 private vlan

As the figure above shows:

All ports are in the private-vlan.

Port 1 is promiscuous port; it can communicate with all other ports.

Port 2 is isolate port; it cannot communicate with all other ports except for the promiscuous port (port 1).

Port 3 and port 4 are community ports in secondary vlan 2; they can communicate with each other. They cannot communicate with all other ports except for the promiscuous port.

Port 5 and port6 are community ports in secondary vlan 3; they can communicate with each other. They cannot communicate with all other ports except for the promiscuous port.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Create a VLAN and configure the port type

```
switch(config)#vlan 1
switch(vlan-1)#private-vlan primary
switch(vlan-1)#private-vlan association 2,3,4
switch(vlan-1)#vlan 2
switch(vlan-2)#private-vlan isolated
switch(vlan-2)#vlan 3
switch(vlan-3)#private-vlan community
switch(vlan-3)#vlan 4
switch(vlan-4)#private-vlan community
```

step 3 Enter the interface configure mode and set the attributes

Promiscuous port： promiscuous port in pvlan can communicate with any other ports in this pvlan

```
switch(config)# interface 10g1/0/1
switch(config-10ge1/0/1)#port link-type access
switch(config-10ge1/0/1)# private-vlan mode promiscuous
switch(config-10ge1/0/1)# private-vlan mapping 1 add 2,3
```

Isolate port： isolate port in pvlan can only communicate with promiscuous port in this pvlan

```
switch(config)# interface 10g1/0/2
switch(config-10ge1/0/2)#port link-type access
switch(config-10ge1/0/2)# private-vlan mode host
switch(config-10ge1/0/2)# private-vlan host-association 1 2
```

Community port： community port in pvlan can communicate with promiscuous port and community ports with same community-vlan id in this pvlan

```
switch(config)# interface 10g1/0/3
switch(config-10ge1/0/3)#port link-type access
switch(config-10ge1/0/3)# private-vlan mode
host
switch(config-10ge1/0/3)# private-vlan host-association 1 3
switch(config)# interface 10g1/0/4
```

```
switch(config-10ge1/0/4)# private-vlan mode host
switch(config-10ge1/0/4)# private-vlan host-association 1 3

switch(config-10ge1/0/5)#port link-type access
switch(config-10ge1/0/5)# private-vlan mode host
switch(config-10ge1/0/5)# private-vlan host-association 1 4

switch(config-10ge1/0/6)#port link-type access
switch(config-10ge1/0/6)# private-vlan mode host
switch(config-10ge1/0/6)# private-vlan host-association 1 4
```

step 4 Exit the configure mode

```
Switch(config)# exit
```

step 5 Validation

The result of show private-vlan is as follows：

```
switch(config)#show private-vlan mapping
  Primary  Sencondary  Type
  1        2           isolated
  1        3           community
  1        4           community
```

6.7.3 Application cases

N/A

6.8 Configuring Port Isolate

6.8.1 Overview

Function Introduction

Port-isolation a security feature which is used to prevent from direct l2/l3 communication among a set of ports.

It can provide a safer and more flexible network solutions by isolating the ports which in the same VLAN.

Generally, it’s used as an access device for user isolation.

Principle Description

N/A

6.8.2 Configuration

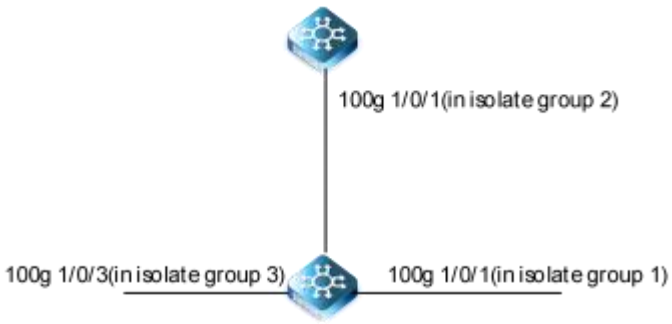


Figure 6-23 Port Isolate

The figure above is the basic topology for port-isolate.

Port 1 and port 8 are in the same isolate group 1, they are isolated. So port1 can not communicate with port 8. Port 9 is in a different isolate group 3, so port 9 can communicate with port 1 and port 8.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Set the port isolate mode globally

The mode "l2" means only layer 2 packets are isolated. The mode "all" means all packet are isolated include the packets forward according to layer 3 routes.

```
Switch(config)# port-isolate mode l2
```

step 3 Configure ports to allow the specified VLAN

```
switch(config)#interface 100g 1/0/1
switch(config-100ge1/0/1)#port hybrid vlan 10 tagged
switch(config-isolate-group1)#exit

switch(config)#interface 100g 1/0/2
switch(config-100ge1/0/1)#port hybrid vlan 10 tagged
switch(config-isolate-group1)#exit

switch(config)#interface 100g 1/0/3
switch(config-100ge1/0/1)#port hybrid vlan 10 tagged
```

step 4 Enter the interface configure mode and set isolate group

```
switch(config-100ge1/0/1)#port-isolate group 1
switch(config-isolate-group1)#add interface 100g
1/0/1 switch(config-isolate-group1)#add interface 100g
```

```
switch(config-100ge1/0/1)#port-isolate group 3
switch(config-isolate-group3)#add interface 100g 1/0/3
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

Use the following command to display the port isolate groups:

```
switch (config)#show port-isolate group
 The interfaces in isolate group 1:
 ------------------------------------------------------------------------------
 100ge1/0/1 100ge1/0/2
 The interfaces in isolate group 3:
 ------------------------------------------------------------------------------
```

6.8.3 100ge1/0/3 Application cases

N/A

7 Device Management Configuration Guide

7.1 Configuring Mirror

7.1.1 Overview

Function Introduction

Mirror function can send one or more copies of packets which are passing through the ports/vlans or sending and receiving by CPU to one or more specified destination ports. It can also send the copies to the CPU and keep in memory or flash files.The copies of the packets are used for network analyze.

The mirror function does not affect the original network traffic.

Principle Description

The following describes concepts and terminology associated with mirror configuration:

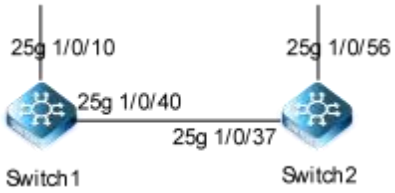


Figure 7-1 Mirror

1.Mirrorsession

A mirror session is a collection of mirror sources and a mirror destination.A working mirror session needs to be configured with the mirror destination and at least one mirror source.

Mirror sessions do not interfere with the normal operation of the switch. However, an oversubscribed mirror destination, for example, a 10-Gbps port monitoring a 100-Gbps port, results in dropped or lost packets.

2.Mirror direction

The device supports to set the direction of the mirror source, there are 3 options for choose: TX/RX/BOTH.

Receive (RX) mirror:

The goal of receive (or ingress) mirror is to monitor as much as possible packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received (except these packets: BPDU, LACPDU, BMGPDU, packets have been discarded by IP-MAC binding check for Vlan_based mirror, CRC error packets for both Port_based and vlan_based mirror) by the source is sent to the destination port for that mirror session. You can monitor a series or range of ingress ports or VLANs in a mirror session. Packets that are modified because of routing are copied without modification; that is, the original packet is copied. Packets that are modified because of quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied with modification. Packets that are modified because of VLAN translation or VLAN classification is copied with the modification. Some features that can cause a packet to be dropped during receive processing have no effect on mirror, the destination port can receive a copy of the packet even if the actual incoming packet is dropped. These features include ingress ACL, VLAN's ingress filter, MAC filter, STP, VLAN tag control, port security, unknown routing packets.

Transmit (TX) mirror:

The goal of transmit (or egress) mirror is to monitor as much as possible packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet (except these packets: packets from CPU port for Vlan_based mirror, mirroring packets for both Port_based and vlan_based mirror) sent by the source is sent to the destination port for that mirror session. Some features that can cause a packet to be dropped during transmit processing might have affect on mirror.

Both:

In a mirror session, you can monitor a single port for both received and sent packets.

3.Mirror source

The Mirror source is the original traffic of the network. The types of source are described as following:

Source port: A source port is a layer2 or layer 2 interface which need to be monitored. A physical port or link agg port can be a source port. The member of link agg port is not supported to be a mirror source.

4.Mirror destination

Mirror function will copy the packets and sent the copies to the mirror destination.

The types of destination are described as following:

Local destination port: The destination port should be a physical port or link agg port, member of link agg port is not supported. The destination port has these characteristics:

- It must reside on the same switch as the source port.
- It should not be in "shutdown" state
- It can participate in only one mirror session at a time (a destination port in one mirror session cannot be a destination port for a second mirror session).
- It cannot be a source port.
- The port does not transmit any traffic except that required for the mirror session.
- It does not participate in spanning tree while the mirror session is active.
- When it is a destination port, all other normal system function of this port should not work until mirror destination configure disabled on this port.
- No address learning occurs on the destination port.
- The real statues of the speed/duplex might not coincide with the values which are displayed.

7.1.2 Configuration

Configuring Local port mirror

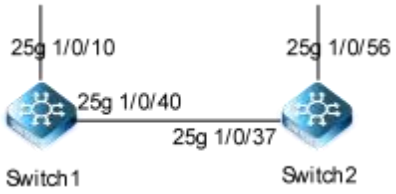


Figure 7-2 port Mirror

Copy the packets of 25g1/0/37 and send them to 100g1/0/56

step 1 Enter the configure mode

```
switch# configure
```

step 2 set the destination of mirror

```
switch1(config)#mirror group 4 100g 1/0/56
```

step 3 Set the source of mirror

```
switch1(config)#interface 25gigaethernet 1/0/37
switch1(config-25ge1/0/37)#mirror ingress group 4
```

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

```
switch1(config)#show mirror config
Version :MIRROR_VX2.10.00.00
!
mirror group 4 100gigaethernet 1/0/56
interface 25ge1/0/37
 mirror ingress group 4
```

7.1.3 Application cases

N/A

7.2 Configuring NTP

7.2.1 Overview

Function Introduction

The Network Time Protocol (NTP) is a networking for clock synchronization between servers and clients. NTP packets are transmitted using UDP port 123.

Principle Description

N/A

7.2.2 Configuration

Configuring NTP Unicast Client/Server Mode

Figure 7-3 NTP Unicast Client/Server Mode

configure the unicast client/server mode to meet the user's requirement for clock synchronization on the LAN

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure reachable routes between switch1 and switch2

Switch1

```
Switch1(config)# vlan 100
Switch1(vlan -100)#int vlanif 100
Switch1(config-vlanif-100)#ip address 192.168.1.1/24
Switch1(config-vlanif-100)#int 10g 1/0/3
Switch1(config-vlanif-100)#port hybrid vlan 100 tagged
Switch1(config-vlanif-100)#int loopback 1
Switch1(config-loopback-1)#ip address 1.1.1.1/24
Switch1(config-loopback-1)#exit
Switch1(config)#router ospf
Switch1(config-ospf-1)#router-id 1.1.1.1
Switch1(config-ospf-1)#network 1.1.1.1 255.255.255.255 area 0
Switch1(config-ospf-1)#network 192.168.1.0 255.255.255.0 area 0
```

Switch2

```
Switch2(config)# vlan 100
```

```
Switch2(vlan -100)#int vlanif 100
Switch2(config-vlanif-100)#ip address 192.168.1.2/24
Switch2(config-vlanif-100)#int 10g 1/0/3
Switch2(config-vlanif-100)#port hybrid vlan 100 tagged
Switch2(config-vlanif-100)#int loopback 1
Switch2(config-loopback-1)#ip address 2.2.2.2/24
Switch2(config-loopback-1)#exit

Switch2(config)#router ospf
Switch2(config-ospf-1)#router-id 2.2.2.2
Switch1(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
Switch1(config-ospf-1)#network 192.168.1.0 255.255.255.0 area 0
```

step 3 Enable the NTP server on switch1, and set the clock stratum to 2

```
Switch1(config)#ntp
Switch1(config-ntp)#master
Switch1(config-ntp)#stratum 2
```

step 4 Specify switch1 as NTP server of switch2

```
Switch2(config)# ntp ntp unicast-server 1.1.1.1
```

Configuring NTP Symmetric Peer Mode

Figure 7-4 NTP Symmetric Peer Mode

The symmetric peer mode is used to synchronize the clocks of Switch1 and Switch2

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure IP address for Switch1 and Switch2

After the configurations are complete, the switches can ping each other

```
Switch1(config)#vlan 100
Switch1(vlan -100)#int vlanif 100
Switch1(config-vlanif-100)#ip address 192.168.1.1/24
Switch1(config-vlanif-100)#int 10g 1/0/3
```

```
Switch1(config-vlanif-100)#port hybrid vlan 100 tagged

Switch2(config)#vlan 100
Switch2(vlan -100)#int vlanif 100
Switch2(config-vlanif-100)#ip address 192.168.1.2/24
Switch2(config-vlanif-100)#int 10g 1/0/3
Switch2(config-vlanif-100)#port hybrid vlan 100 tagged
```

step 3 Configure the NTP unicast symmetric peer mode

```
Switch1(config)#ntp
Switch1(config-ntp)#ntp unicast-peer 192.168.1.2
```

step 4 Set the clock stratum, make the switch1 synchronize its clock with the clock of switch2

Set the clock stratum to 3 on switch1

```
Switch1(config)#ntp
Switch1(config-ntp)#stratum 3
```

Set the clock stratum to 2 on switch2

```
Switch2(config)#ntp
Switch2(config-ntp)#stratum 2
```

Configuring NTP multicast Mode

Figure 7-5 NTP Multicast Mode

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure IP address for Switch1 and Switch2

After the configurations are complete, the switches can ping each other

```
Switch1(config)#vlan 100
Switch1(vlan -100)#int vlanif 100
Switch1(config-vlanif-100)#ip address 192.168.1.1/24
Switch1(config-vlanif-100)#int 10g 1/0/3
Switch1(config-vlanif-100)#port hybrid vlan 100 tagged
```

```
Switch2(config)#vlan 100
Switch2(vlan -100)#int vlanif 100
Switch2(config-vlanif-100)#ip address 192.168.1.2/24
Switch2(config-vlanif-100)#int 10g 1/0/3
Switch2(config-vlanif-100)#port hybrid vlan 100 tagged
```

step 3 Configure the NTP multicast mode

Configure Switch1 as the NTP multicast server

```
Switch1(config)#ntp
Switch1(config-ntp)#stratum 2
Switch1(config-ntp)#int vlan 100
Switch1(config-vlanif-100)#ntp multicast-server
```

Configure Switch2 as the NTP multicast client

```
Switch2(config)#int vlan 100
Switch2(config-vlanif-100)#ntp multicast-client
```

Configuring NTP broadcast Mode

Figure 7-5 NTP broadcast Mode

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure IP address for Switch1 and Switch2

After the configurations are complete, the switches can ping each other

```
Switch1(config)#vlan 100
Switch1(vlan -100)#int vlanif 100
Switch1(config-vlanif-100)#ip address 192.168.1.1/24
Switch1(config-vlanif-100)#int 10g 1/0/3
Switch1(config-vlanif-100)#port hybrid vlan 100 tagged

Switch2(config)#vlan 100
Switch2(vlan -100)#int vlanif 100
Switch2(config-vlanif-100)#ip address 192.168.1.2/24
Switch2(config-vlanif-100)#int 10g 1/0/3
Switch2(config-vlanif-100)#port hybrid vlan 100 tagged
```

step 3 Configure the NTP broadcast mode

Configure Switch1 as the NTP broadcast server

```
Switch1(config)#ntp
Switch1(config-ntp)#stratum 2
Switch1(config-ntp)#int vlan 100
Switch1(config-vlanif-100)#ntp broadcast-server
```

Configure Switch2 as the NTP multicast client

```
Switch2(config)#int vlan 100
Switch2(config-vlanif-100)#ntp broadcast-client
```

7.3 Configuring Device Management

7.3.1 Overview

Function Introduction

User can manage the switch through the management port. The switch has two management ports: an Ethernet port and a console port.

Principle Description

N/A

7.3.2 Configuration

Configuring out-of-band Ethernet port for management

In order to manage device by out band Ethernet port, you should configure management ip address first by console port.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Configure switch management address

IPv4 & IPv6 are both supported, for example:

```
switch1(config)#interface mgt-eth 0/0/0
switch1(config-mgt-eth-0/0/0)# ip address 10.32.133.120/23
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch1(config)#int mgt-eth 0/0/0
switch1(config-mgt-eth-0/0/0)#show
!
interface mgt-eth 0/0/0
 ip address 10.32.133.120/23
```

Configuring Temperature

The switch supports temperature alarm management. You can configure three temperature thresholds: low, high and critical. When switch temperature is lower than low threshold or higher than higher threshold, the switch will be alarm. If the switch temperature is higher than critical threshold,the switch will cut off its power automatically.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Configuring temperature threshold

-10℃ for low;60℃ for high;

```
switch1(config)#temperature monitor enable
switch1(config)#temperature  all low-threshold -10 high-threshold 60
```

step 3 Exit the configure mode

```
switch(config)#end
```

step 4 Validation

```
switch1(config)#show temperature
Temperature information:
 Temperature monitor:enable
    Index            CurrValue L-Threshold H-Threshold Status        Trap          Descr
*   Temper-1/0/1     34        -10         60          normal        enable        Sensor Temperature
```

Configuring Fan

The switch supports to manage fan automatically. If the fan is fail or the fan tray is absent,the switch will be alarm. And if the fan is OK,the switch can adjust the fan speed depending on the real-time temperature.

```
switch1#show fan
Fan information:
 Fan monitor:enable
    FanCtrl          Speed   Level  L-Threshold H-Threshold Status        Trap      Mode                Serial      Descr
*   Fan-1/1          8500    4      200         15000       normal        enable    temperature-ctrl    N/A         CTRL-1/1
*   Fan-1/2          8300    4      200         15000       normal        enable    temperature-ctrl    N/A         CTRL-1/2
```

*	Fan-1/3	8500	4	200	15000	normal	enable	temperature-ctrl	N/A	CTRL-1/3
*	Fan-1/4	8400	4	200	15000	normal	enable	temperature-ctrl	N/A	CTRL-1/4
*	Fan-1/5	8400	4	200	15000	normal	enable	temperature-ctrl	N/A	CTRL-1/5
*	Fan-1/6	8400	4	200	15000	normal	enable	temperature-ctrl	N/A	CTRL-1/6

7.3.3 Application cases

N/A

8 Network Management Configuration Guide

8.1 Configuring RMON

8.1.1 Overview

Function Introduction

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switched on all connected LAN segments.

RMON is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

Principle Description

N/A

8.1.2 Configuration

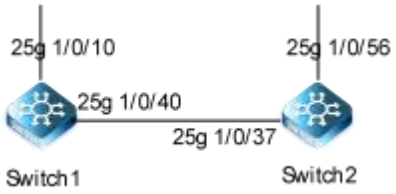


Figure 8-1 rmon

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode and create a stats and a history

```
switch2(config)#int 25g 1/0/37
switch2(config-25ge1/0/37)# rmon statistics 1
switch2(config-25ge1/0/37)# rmon history 1 10 20
```

step 3 Create an event with log and trap both set.

```
switch2(config)#rmon event 1 both
```

step 4 Create a alarm and count it every 1000 seconds. Event 1 will be triggered if it goes above 20,000 or below 1000

```
switch2(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.10.4390 30 absolute 20000 1 1000 1
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

```
switch2(config)#show rmon config
!
rmon event 1 both
rmon alarm 1 1.3.6.1.2.1.2.2.1.10.4390 30 absolute 20000 1 1000 1
!
interface 25gigaethernet 1/0/37
 rmon statistics 1
 rmon history 1 10 20

switch2(config-25ge1/0/16)#show rmon statistic
  RMON Ethernet statistics 1
    Data Source:ifIndex.25ge1/0/37
    Owner: N/A
    Status: valid
    Rx statistics:
        Octets:0/45100636
        Pkts: 0/644275
        Broadcast: 0/1
        Multicast: 0/48
    Packets statistics:
        64 Octets: 0/1
        65-127 Octets: 0/644273
        128-255 Octets: 0/2
        256-511 Octets: 0/0
        512-1023 Octets: 0/0
        1024-1518 Octets: 0/0
        Jabbers: 0/0
            Error statistics:
        CRC Errors: 0/0
        Undersize: 0/0
        Oversize: 0/0
        Fragments: 0/0
        Collisions: 0/0

switch2(config-25ge1/0/16)#show rmon history
  'BR' means 'Buckets Requested'
  'BG' means 'Buckets Granted'
  'DS' means 'Data Source'
  'ACT' means 'Active
  'UC' means 'Undercreation'
  RMON ethernet statistics
```

```
  Index BR      BG      Interval State DS
  1     20      20      10       ACT   ifIndex.25ge1/0/37

switch2(config-25ge1/0/16)#show rmon event
  RMON Event:1
        Type:trap&log
        Status:valid
        Lastsent time:4 days 17 hours 53 minutes 37 seconds
        Description:N/A
        Owner:N/A

switch2(config-25ge1/0/16)#show rmon alarm
  RMON Alarm:1
        Interval:30
        SourceOID:1.3.6.1.2.1.2.2.1.10.4390
        Sample Type:absolute value
        Alarm Value:86731836
        Startup Alarm:risingOrFallingAlarm
        Rising Threshold:20000
        Rising Event:1
        Falling Threshold:1000
        Falling Event:1
        Owner:N/A
        Status:valid

switch2(config)#show rmon log
  RMON Log:1/1
        Time:4 days 17 hours 53 minutes 37 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.10.4390,1,2905192185,20000
```

8.1.3 Application cases

N/A

8.2 Configuring SNMP

8.2.1 Overview

Function Introduction

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS). The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent. The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data. An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a

condition on the network. Error user authentication, restarts, link status (up or down), MAC address tracking, closing of a Transmission Control Protocol (TCP) connection, loss of connection to a neighbor, or other significant events may send a trap.

Principle Description

SNMP module is based on the following RFC draft:

- **SNMPv1 :** Defined in RFC 1157.
- **SNMPv2C :** Defined in RFC 1901.
- **SNMPv3 :** Defined in RFC 2273 to 2275.

Following is a brief description of terms and concepts used to describe the SNMP protocol:

- **Agent :** A network-management software module, an agent has local knowledge of management information and translates that information into a form compatible with SNMP.
- **Management Information Base (MIB) :** Management Information Base, collection of information is organized hierarchically.
- **Engine ID :** A unique ID for a network's node.
- **Trap :** Used by managed devices to asynchronously report events to the NMS.

8.2.2 Configuration

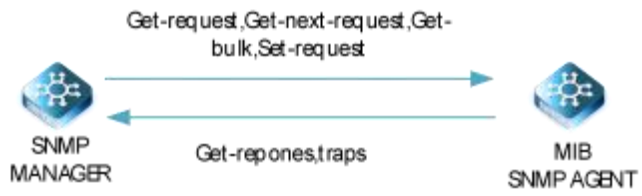


Figure 8-2 snmp

As shown in the figure SNMP agent gathers data from the MIB. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps alert the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in get-request, get-next-request, and set-request format.

Configuring community string

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. Optionally, you can specify one or more of these characteristics associated with the string:

- A MIB view, which difines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community

Follow these steps to configure a group string on the switch, and once configured, you can implement the basic read and write functions of SNMP.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Configure community

Configure a view name (optional).Configure the group name "pub" for read and write permissions.

```
switch(config)#snmp view v1 1.3.6.1.2 include
switch(config)#snmp community pub rw view v1
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch2(config)#show snmp   config
 Software Version                    :SNMP_VX2.11.03.00
!
snmp version v1
snmp contact syscontact1
snmp view r1 1.3.6 included
snmp view r1 1.3.6.1.2.1.1.2 excluded
snmp view v1 1.3.6.1.2 included
snmp community $9$kijv$dc3761dfeac4bd85 rw cipher view v1
no snmp community private
```

Configuring SNMPv3 Groups,Users and Accesses

You can specify an identification name (engine ID) for the local SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, you can add new users to the SNMP group, and you can add access for the SNMP group.

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the switch.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Set the globle configurations for SNMP

Set engineID; Set the user name, password, and authentication type; Create SNMP server; Set the authority for the group member.

```
switch(config)#snmp user hjr group g1 auth md5 12345 priv des 12345
switch(config)#snmp view r1 1.3.6 included
switch(config)#snmp view r1 1.3.6.1.2.1.1.2 excluded
```

```
switch(config)#snmp group g1 read-view r1 write-view internet notify-view internet
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch2(config)#show snmp config
 Software Version                :SNMP_VX2.11.03.00
!
snmp version v3
snmp contact syscontact1
snmp view r1 1.3.6 included
snmp view v1 1.3.6.1.2 included
snmp community $9$kijv$dc3761dfeac4bd85 rw cipher view v1
no snmp community private
snmp trap-server 172.100.10.165 162 hjr v3
snmp group g1 read-view r1 write-view internet notify-view internet
snmp user hjr group g1 auth md5 0x67bffd5ccf2087cf71fdb5dcd5bf9c3b priv des 0x67bffd5ccf2087cf71fdb5dcd5bf9c3b
```

SNMPv1 and SNMPv2 trap configure

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the switch.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Set the global configurations for SNMP

Configure the destination address and the group name pub

```
switch(config)#snmp trap-server 172.100.10.165 162 pub v1
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch(config)#show snmp   config
 Software Version                :SNMP_VX2.11.03.00
!
snmp version v1
snmp contact syscontact1
snmp view r1 1.3.6 included
```

```
snmp view r1 1.3.6.1.2.1.1.2 excluded
snmp view v1 1.3.6.1.2 included
snmp community $9$kijv$dc3761dfeac4bd85 rw cipher view v1
no snmp community private
snmp trap-server 172.100.10.165 162 pub v1
```

Configuring SNMPv3 trap

step 1 Enter the configure mode

```
switch# configure
```

step 2 Set the global configurations for SNMP

Create a Trap message entry;Configure destination IPv4 addresses and user names;Join a user to the SNMP group.

```
switch(config)#snmp user hjr group g1 auth md5 12345 priv des 12345
switch(config)#snmp view r1 1.3.6 included
switch(config)#snmp view r1 1.3.6.1.2.1.1.2 excluded
switch(config)#snmp group g1 read-view r1 write-view r1 notify-view r1
switch(config)#snmp trap-server 172.100.10.165 162 hjr v3
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch (config)#show snmp   config
Software Version                    :SNMP_VX2.11.03.00
!
snmp version v3
snmp contact syscontact1
snmp view r1 1.3.6 included
snmp view r1 1.3.6.1.2.1.1.2 excluded
snmp view v1 1.3.6.1.2 included
snmp community $9$kijv$dc3761dfeac4bd85 rw cipher view v1
no snmp community private
snmp trap-server 172.100.10.165 162 hjr v3
snmp trap-server 172.100.10.165 162 pub v1
snmp group g1 read-view r1 write-view r1 notify-view r1
snmp user hjr group g1 auth md5 0x67bffd5ccf2087cf71fdb5dcd5bf9c3b priv des 0x67bffd5ccf2087cf71fdb5dcd5bf9c3b
```

8.2.3 Application cases

N/A

8.3 Configuring LLDP

8.3.1 Overview

Function Introduction

LLDP （ Link Layer Discovery Protocol ） is the discovery protocol on link layer defined as standard in IEEE 802.1ab. Discovery on Layer 2 can locate interfaces attached to the devices exactly with connection information on layer 2, such as VLAN attribute of port and protocols supported, and present paths among client, switch, router, application servers and other network servers. This detailed description is helpful to get useful information for diagnosing network fast, like topology of devices attached, conflict configuration between devices, and reason of network failure.

Principle Description

N/A

8.3.2 Configuration

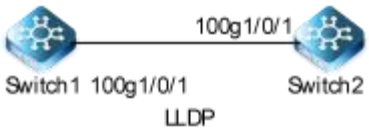


Figure 8-3 lldp

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode and set the attributes of LLDP on the interface

```
switch1:
Switch1(config)# interface 10g1/0/1
switch1(config-10ge1/0/1)#interface 10gigaethernet 1/0/1
Switch1(config-10ge1/0/1)#lldp admin-status rx-tx


Switch2:
Switch2(config)# interface 10g1/0/1
switch2(config-10ge1/0/1)#interface 10gigaethernet 1/0/1
switch2(config-10ge1/0/1)#lldp admin-status rx-tx
```

step 3 Enable Notification on the interface

```
switch1:
switch1(config)# interface 10g1/0/1
switch1(config-10ge1/0/1)#interface 10gigaethernet 1/0/1
Switch1(config-10ge1/0/1)#lldp notification enable
Switch2:
Switch2(config)# interface 10g1/0/1
```

```
switch2(config-10ge1/0/1)#interface 10gigaethernet 1/0/1
Switch2(config-10ge1/0/1)#lldp notification enable
```

step 4 Exit the configure mode

```
Switch(config)# end
```

step 6 Verify the configuration

To display the LLDP neighbor , use following command:

```
Switch1# show lldp local config
switch1(config)#show lldp remote
Remote system information:
Interface       Index TTL(s)  ChassId              PortId                SysName
10ge1/0/1       1     110     80a2:3546:4fc9       10GigaEthernet1/0/1   switch2
mgt-eth0/0/0    2     99      649d:991f:0202       Eth 1/28              -

Switch2#show lldp remote
Remote system information:
Interface       Index TTL(s)  ChassId              PortId                SysName
10ge1/0/1       1     107     6821:5fcf:f9c2       10GigaEthernet1/0/1   Switch1
mgt-eth0/0/0    2     101     649d:991f:0202       Eth 1/30              -
```

9 Traffic Managemant Configuration Guide

9.1 Configuring QoS

9.1.1 Overview

Function Introduction

QoS (Quality of Service) is a common concept in various situations where there is a Service supply and demand relationship. It evaluates the Service side's ability to meet customer Service demands.Evaluation is usually not an accurate score, but rather an analysis of what conditions the service is good under and where it is deficient in order to make targeted improvements.In the Internet, QoS evaluates the service capability of network delivery groups.Since the services offered by the network are diverse, the evaluation of QoS can be based on different aspects.The QoS commonly referred to is the assessment of the service capability that provides support for the core requirements such as delay, delay jitter and packet loss rate during packet delivery.QoS is a security mechanism of network and a technology used to solve the problem of network delay and blocking.Under normal circumstances, QoS is not required if the network is only used for certain time-limited applications, such as Web applications, or E-mail Settings.But it is essential for critical and multimedia applications.When the network is overloaded or congested, QoS can ensure that the important traffic is not delayed or discarded, while ensuring the efficient operation of the network.

Principle Description

Following is a brief description of terms and concepts used to describe QoS：

ACL

Access control lists (ACLs) classify traffic with the same characteristics. IP traffic is classified using IP ACLs, and non-IP traffic is classified using MAC ACLs. The ACL can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet.

CoS Value

Class of Service (CoS) is a 3-bit value used to classify the priority of Layer-2 frames upon entry into a network.

QoS classifies frames by assigning priority-indexed CoS values to them, and gives preference to higher-priority traffic.

Layer-2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS values in the 3 most significant bits, called the User Priority bits. On interfaces configured as Layer-2 802.1Q trunks, all traffic is in 802.1Q frames, except for traffic in the native VLAN.

Other frame types cannot carry Layer-2 CoS values. CoS values range from 0 to 7.

DSCP Value

Differentiated Services Code Point (DSCP) is a 6-bit value used to classify the priority of Layer-3 packets upon entry into a network.

DSCP values range from 0 to 63.

IP-Precedence Value

IP-Precedence is a 3-bit value used to classify the priority of Layer-3 packets upon entry into a network.

IP-Precedence values range from 0 to 7.

EXP Value

EXP value is a 3-bit value used to classify the priority of MPLS packets upon entry into a network.

MPLS EXP values range from 0 to 7.

Traffic Classification

QoS (Quality of Service) is a common concept in various situations where there is a Service supply and demand relationship. It evaluates the Service side's ability to meet customer Service demands.Evaluation is usually not an accurate score, but rather an analysis of what conditions the service is good under and where it is deficient in order to make targeted improvements.In the Internet, QoS evaluates the service capability of network delivery groups.Since the services offered by the network are diverse, the evaluation of QoS can be based on different aspects.The QoS commonly referred to is the assessment of the service capability that provides support for the core requirements such as delay, delay jitter and packet loss rate during packet delivery.QoS is a security mechanism of network and a technology used to solve the problem of network delay and blocking.Under normal circumstances, QoS is not required if the network is only used for certain time-limited applications, such as Web applications, or E-mail Settings.But it is essential for critical and multimedia applications.When the network is overloaded or congested, QoS can ensure that the important traffic is not delayed or discarded, while ensuring the efficient operation of the network.

Shaping

Shaping is to change the rate of incoming traffic flow to regulate the rate in such a way that the outgoing traffic flow behaves more smoothly. If the incoming traffic is highly bursty, it needs to be buffered so that the output of the buffer is less bursty and smoother.

Shaping has the following attributes:

- Shaping can be deployed base on physical port.
- Shaping can be deployed on queues of egress interface.

When queue applies dual rate shaping, it is necessary to ensure that the sum of CIR of all queues under the interface is not greater than the port rate and that is not greater than the rate of shaping in the interface.

Policing

Policing determines whether a packet is in or out of profile by comparing the internal priority to the configured policer.

The policer limits the bandwidth consumed by a traffic flow. The result is given to the marker.

There are two types of policers:

- Individual: QoS applies the bandwidth limits specified in the policer, separately, to each matched traffic class. An individual policer is configured within a policy map.

- Aggregate: QoS applies the bandwidth limits specified in an aggregate policer, cumulatively, to all matched traffic flows. An aggregate policer is configured by specifying the policer name within a policy map. The bandwidth limits of the policer are specified. In this way, the aggregate policer is shared by multiple classes of traffic within one or multiple policy map.

Marking

Marking determines how to handle a packet when it is out of profile. It assesses the policer and the configuration information to determine the action required for the packet, and then handles the packet using one of the following methods:

- Let the packet through and mark color down
- Drop the packet

Marking can occur on ingress and egress interfaces.

Queuing

Queuing maps packets to a queue. Each egress port can accommodate up to 8 unicast queues, 4 multicast queues and 1 SPAN queue.

The packet internal priority can be mapped to one of the egress queues. The unit of queue depth is buffer cell. Buffer cell is the granularity, which is 288 bytes, for packet storing.

After the packets are mapped to a queue, they are scheduled.

Tail Drop

Tail drop is the default congestion-avoidance technique on the interface. With tail drop, packets are queued until the thresholds are exceeded. The packets with different priority and color are assigned to different drop precedence. The mapping between priority and color to queue and drop precedence is configurable. You can modify the three tail-drop threshold to every egress queue by using the queue threshold interface configuration command. Each threshold value is packet buffer cell, which ranges from 0 to 16383.

Scheduling

Scheduling forwards conditions packets using combination of WDRR and SP. Every queue belongs to a class. The class range from 0 to 7, and 7 is the highest priority. Several queues can be in a same class, or non queue in some class. Packets are scheduled by SP between classes and WDRR between queues in a class.

- Strict Priority-Based (SP), in which any high-priority packets are first transmitted. Lower-priority packets are transmitted only when the higher-priority queues are empty. A problem may occur when too many lower-priority packets are not transmitted.
- Weighted Deficit Round Robin (WDRR), in which each queue is assigned a weight to control the number of packets relatively sent from each queue.

Time-range

By using time-range, the aces in the class-map can be applied based on the time of day or week. First, define a time-range name and set the times and the dates or the days of the week in the time range. Then enter the time-range name when adding an ace.

You can use the time-range to define when the aces in the class-map are in effect, for example, during a specified time period or on specified days of the week.

RTCM

Single Rate Three Color Marker

TRTCM

Two Rate Three Color Marker

CIR

Committed Information Rate

CBS

Committed Burst Size

EBS

Excess Burst Size

PIR

Peak Information Rate

9.1.2 Configuration for qos policy-map

The following steps are required when deploying the QoS traffic policy.

- Identify and differentiate traffic to different categories
- Configure policies for different traffic categories.
- application strategies on the interface.

Modify message priority and car policy speed limits

The following example shows how to create a policy table to classify, mark, and limit traffic.In this example, a policy table is created and applied to the import traffic on a port.The configured IP ACL allows traffic from the 10.1.00 address to be discarded if their average rate exceeds 48,000 - KBPS.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create the ACL

```
switch1(config)# filter-list 1500
switch1(configure-filter-ipv4-1500)# filter 5 ip any 20.1.30.0/24
switch1(configure-filter-ipv4-1500)# filter 5 action priority 3
switch1(configure-filter-ipv4-1500)#
switch1(configure-filter-ipv4-1500)# filter 10 ip any any dscp 3
switch1(configure-filter-ipv4-1500)# filter 10 action dscp cs5
switch1(configure-filter-ipv4-1500)#
switch1(configure-filter-ipv4-1500)# filter 15 ip 20.1.20.3/24 any
switch1(configure-filter-ipv4-1500)# filter 15 car 5000000 outaction drop
```

step 3 Enter the interface configure and apply the policy table

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#filter-list in 1500
switch1(config-100ge1/0/25)#
```

Note ： The interface allows only one policy map to be configured per direction.

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

```
switch1(config)#show filter-list config

 filter-list 1500 filter 3
 filter-list 1500
 filter 5 ip any 20.1.30.0/24
 filter 5 action priority 3

 filter 10 ip any any dscp 3
 filter 10 action dscp cs5

 filter 15 ip 20.1.20.3/24 any
 filter 15 car 5000000 outaction drop



 interface 100ge1/0/25
 filter-list in 1500
```

The speed limit template is called to limit the speed

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create ACL and ACEs

```
switch1(config)# filter-list 1500
switch1(config)#meter 1 cir 1000000 cbs 2000000 pbs 4000000 pir 2000000 blind
switch1(config)# filter-list 1600
switch1(configure-filter-ipv4-1600)# filter 1 ip any 20.1.30.0/24
switch1(configure-filter-ipv4-1600)# filter 1 meter 1
switch1(configure-filter-ipv4-1600)# filter 1 outaction red drop
```

step 3 Enter the interface configure and apply the policy table

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#filter-list in 1600t
```

Note： the interface allows only one policy map to be configured per direction.

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

```
switch1(config)#show meter config
!
meter 1 cir 1000000 cbs 2000000 pbs 4000000 pir 2000000 blind

switch1(config)#show filter-list config

 filter-list 1500 filter 3
 filter-list 1500
 filter 5 ip any 20.1.30.0/24
 filter 5 action priority 3

 filter 10 ip any any dscp 3
 filter 10 action dscp cs5

 filter 15 ip 20.1.20.3/24 any
 filter 15 car 5000000 outaction drop
```

```
interface 100ge1/0/25
filter-list in 1500
```

Specifies that the business flow goes to the appropriate queue

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create ACL and ACEs

```
switch1(config)# filter-list 1600
switch1(configure-filter-ipv4-1600)#filter 5 ip 20.1.20.5/24 20.1.50.5/24
switch1(configure-filter-ipv4-1600)#filter 5 action cos 6
```

step 3 Enter the interface configure and apply the policy table

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#filter-list in 1600
```

Note： the interface allows only one policy map to be configured per direction.

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

```
switch1#show filter-list config

filter-list 1600 filter 1
filter-list 1600
filter 5 ip 20.1.20.5/24 20.1.50.5/24
filter 5 action cos 6

interface 100ge1/0/25
filter-list in 1600
```

Redirects to the specified interface

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create ACL and ACEs

```
switch1(config)#mirror group 1 100gigaethernet 1/0/1
switch1(config)# filter-list 1600
switch1(configure-filter-ipv4-1600)#filter 10 ip any 30.1.1.0/24
switch1(configure-filter-ipv4-1600)#filter 10 action mirror group 1
```

step 3 Enter the interface configure and apply the policy table

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#filter-list in 1600
```

Note： the interface allows only one policy map to be configured per direction.

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

```
Switch# show qos aggregate-policer
Aggreate policer: transmit1
   color blind
   CIR 48000 kbps, CBS 8000 bytes, EBS 10000 bytes
   drop violate packets
switch1#show mirror config
Version :MIRROR_VX2.10.00.00
!
mirror group 1 100gigaethernet 1/0/1

switch1#show filter-list config

 filter-list 1500 filter 1
 filter-list 1500
 filter 10 ip any 30.1.1.0/24
 filter 10 action mirror group 1
interface 100ge1/0/25
 filter-list in 1600
switch1#
```

9.1.3 Configuration for Queue

Configuring Sp Quene Schedule

step 1 Enter the configure mod

```
switch# configure
```

step 2 Enter the interface configure mode and configure sp schedul

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#cos scheduling sp
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch1(config-100ge1/0/25)#show cos interface 100g 1/0/25
  scheduling algorithm is sp
  'BW' means 'Bandwidth'
  'bps' means 'bits per second'
```

Interface	Queue	Max-BW(bps)	Min-BW(bps)	Weight
100ge1/0/25	0	0M	0M	N/A
100ge1/0/25	1	0M	0M	N/A
100ge1/0/25	2	0M	0M	N/A
100ge1/0/25	3	0M	0M	N/A
100ge1/0/25	4	0M	0M	N/A
100ge1/0/25	5	0M	0M	N/A
100ge1/0/25	6	0M	0M	N/A
100ge1/0/25	7	0M	0M	N/A

```
switch1(config)#show cos config
interface 100gigaethernet 1/0/25
```

Configuring RR Quene Schedule

step 1 Enter the configure mod

```
switch# configure
```

step 2 Enter the interface configure mode and configure rr schedul

```
switch1(config)#int 100g 1/0/25
```

```
switch1(config-100ge1/0/25)#cos scheduling rr
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch1(config)#show cos interface 100g 1/0/25
  scheduling algorithm is rr
  'BW' means 'Bandwidth'
  'bps' means 'bits per second'
```

Interface	Queue	Max-BW(bps)	Min-BW(bps)	Weight
100ge1/0/25	0	0M	0M	N/A
100ge1/0/25	1	0M	0M	N/A
100ge1/0/25	2	0M	0M	N/A
100ge1/0/25	3	0M	0M	N/A
100ge1/0/25	4	0M	0M	N/A
100ge1/0/25	5	0M	0M	N/A
100ge1/0/25	6	0M	0M	N/A

Configuring WRR Quene Schedule

step 1 Enter the configure mod

```
switch# configure
```

step 2 Enter the interface configure mode and configure wrr schedul

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#cos scheduling wrr
switch1(config-100ge1/0/25)#cos queue 0-1 weight 4
switch1(config-100ge1/0/25)#cos queue 2-4 weight 6
switch1(config-100ge1/0/25)#cos queue 5-7 weight 8
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch1(config-100ge1/0/25)#show cos interface 100g 1/0/25
  scheduling algorithm is wrr
  'BW' means 'Bandwidth'
  'bps' means 'bits per second'
```

Interface	Queue	Max-BW(bps)	Min-BW(bps)	Weight

100ge1/0/25	0	0M	0M	4
100ge1/0/25	1	0M	0M	4
100ge1/0/25	2	0M	0M	6
100ge1/0/25	3	0M	0M	6
100ge1/0/25	4	0M	0M	6
100ge1/0/25	5	0M	0M	8
100ge1/0/25	6	0M	0M	8
100ge1/0/25	7	0M	0M	8

```
switch1(config-100ge1/0/25)#show cos config

interface 100gigaethernet 1/0/25
 cos scheduling wrr
 cos queue 0-1 weight 4
 cos queue 2-4 weight 6
 cos queue 5-7 weight 8
```

Configuring DRR Quene Schedule

step 1 Enter the configure mod

```
switch# configure
```

step 2 Enter the interface configure mode and configure drr schedul

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#cos scheduling drr
switch1(config-100ge1/0/25)# cos queue 0-1 weight 4
switch1(config-100ge1/0/25)# cos queue 2-4 weight 6
switch1(config-100ge1/0/25)# cos queue 5-7 weight 8
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch1(config)#show cos interface 100g 1/0/25
  scheduling algorithm is drr
  'BW' means 'Bandwidth'
  'bps' means 'bits per second'
```

Interface	Queue	Max-BW(bps)	Min-BW(bps)	Weight
100ge1/0/25	0	0M	0M	4
100ge1/0/25	1	0M	0M	4
100ge1/0/25	2	0M	0M	6
100ge1/0/25	3	0M	0M	6
100ge1/0/25	4	0M	0M	6

100ge1/0/25	5	0M	0M	8
100ge1/0/25	6	0M	0M	8
100ge1/0/25	7	0M	0M	8

Configuring SP+WRR Quene Schedule

step 1 Enter the configure mod

```
switch# configure
```

step 2 Enter the interface configure mode and configure SP+DRR schedul,and quene 5,6,7configure mode sp

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#cos scheduling sp+wrr 5-7
switch1(config-100ge1/0/25)# cos queue 0-1 weight 4
switch1(config-100ge1/0/25)# cos queue 2-4 weight 6
```

step 3 Exit the configure mode

```
switch(config)# end
```

step 4 Validation

```
switch1(config)#show cos interface 100g 1/0/25
  scheduling algorithm is sp+wrr,queue list 5-7
  'BW' means 'Bandwidth'
  'bps' means 'bits per second'
```

Interface	Queue	Max-BW(bps)	Min-BW(bps)	Weight
100ge1/0/25	0	0M	0M	4
100ge1/0/25	1	0M	0M	4
100ge1/0/25	2	0M	0M	6
100ge1/0/25	3	0M	0M	6
100ge1/0/25	4	0M	0M	6
100ge1/0/25	5	0M	0M	N/A
100ge1/0/25	6	0M	0M	N/A
100ge1/0/25	7	0M	0M	N/A

Queue shaping

step 1 Enter the configure mod

```
switch# configure
```

step 2 Enter the interface configure mode and configure sp+wrr schedul,and quene 5,6,7configure mode sp

```
switch1(config)#int 100g 1/0/25
```

```
switch1(config-100ge1/0/25)#cos scheduling sp+wrr 5-7
switch1(config-100ge1/0/25)# cos queue 0-1 weight 4
switch1(config-100ge1/0/25)# cos queue 2-4 weight 6
```

step 3 nter the interface configure mode and configure shaping for quene 5,6.7

```
switch1(config)#int 100g 1/0/25
switch1(config-100ge1/0/25)#cos queue 5 min-bandwidth gbps 1
switch1(config-100ge1/0/25)#cos queue 6 min-bandwidth gbps 1
switch1(config-100ge1/0/25)#cos queue 7 min-bandwidth gbps 1
switch1(config-100ge1/0/25)#cos queue 5 max-bandwidth gbps 5
switch1(config-100ge1/0/25)#cos queue 6 max-bandwidth gbps 5
switch1(config-100ge1/0/25)#cos queue 7 max-bandwidth gbps 5
```

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

```
switch1#show cos interface 100g 1/0/25
 scheduling algorithm is sp+wrr,queue list 5-7
 'BW' means 'Bandwidth'
 'bps' means 'bits per second'
```

Interface	Queue	Max-BW(bps)	Min-BW(bps)	Weight
100ge1/0/25	0	0M	0M	4
100ge1/0/25	1	0M	0M	4
100ge1/0/25	2	0M	0M	6
100ge1/0/25	3	0M	0M	6
100ge1/0/25	4	0M	0M	6
100ge1/0/25	5	5G	1G	N/A
100ge1/0/25	6	5G	1G	N/A
100ge1/0/25	7	5G	1G	N/A

9.1.4 Application cases

N/A

10 IPv6 Service Configuration

10.1 Configuring ND

10.1.1 Overview

Function Introduction

Nodes (hosts and routers) use Neighbor Discovery to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid.

Hosts also use Neighbor Discovery to find neighboring routers that are willing to forward packets on their behalf.

Finally, nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses. When a router or the path to a router fails, a host actively searches for functioning alternates.

Principle Description

N/A

10.1.2 Configuration

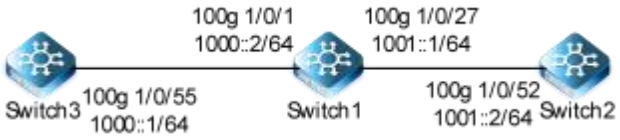


Figure10-1 NDP

In this example,The aging time was configured for 10min,interface 100g1/0/27 assigned with static ndp 1000::2/64

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode and set the attributes of the interface

```
switch3(config)#vlan 1000
switch3(config-100ge1/0/55)#port link-type trunk
switch3(config-100ge1/0/55)#port trunk allow-pass vlan
1000 switch3(config-100ge1/0/55)#int vlan 1000
switch3(config-vlanif-1000)#ipv6 enable
switch3(config-vlanif-1000)#ipv6 address 1000::1/64
switch3(config-vlanif-1000)#quit
```

Switch1

```
switch1(config)#vlan 1000-1001
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#port link-ty trunk
switch1(config-100ge1/0/31)#port trunk allow-pass vlan
```

```
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port trunk allow-pass vlan 1001

switch1(config-100ge1/0/27)#int vlan 1000
switch1(config-vlanif-1000)#ipv6 enable
switch1(config-vlanif-1000)#ipv6 address 1000::2/64
switch1(config-vlanif-1000)#quit
switch1(config)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 enable
switch1(config-vlanif-1001)#ipv6 address 1001::1/64
switch1(config-vlanif-1001)#quit

Switch2
switch2(config)#vlan 1001
switch2(vlan-1001)#int 100g 1/0/52
switch2(config-100ge1/0/52)#port link-type trunk
switch2(config-100ge1/0/52)#port trunk allow-pass vlan 1001
switch2(config-100ge1/0/52)#int vlan 1001
switch2(config-vlanif-1001)#ipv6 enable
switch2(config-vlanif-1001)#ipv6 address 1001::2/64
switch2(config-vlanif-1001)#quit
```

step 3 configured the aging time

```
switch1(config)#ipv6 nd lifetime 600
```

step 4 Configure static neighbor table entries

```
switch1(config)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 neighbor    1001::2 68:21:5F:B7:5B:10 100g 1/0/27
```

step 5 Exit the configure mode

```
switch(config)# end
```

step 6 Validation

```
switch1(config)#show ipv6 neighbor
  Neighbor aging time: 600(s)
  IPv6Addr                                L2Addr              Interface          State      Aging      Type       Vpn-
instance
  ------------------------------------------------------------------------------------------------------------------
  1000::1                                 68:21:5F:DB:FC:00   100ge1/0/31        Reachable  546        Dynamic    N/A
  1000::2                                 68:21:5F:FB:0F:54   vlan1000           Reachable  never      Local      N/A
  1001::1                                 68:21:5F:FB:0F:54   vlan1001           Reachable  never      Local      N/A
  1001::2                                 68:21:5F:B7:5B:10   100ge1/0/27        Reachable  never      Static     N/A
  fe80:3ac::6a21:5fff:fefb:f54            68:21:5F:FB:0F:54   vlan1000           Reachable  never      Local      N/A
```

```
fe80:3ad::6a21:5fff:fefb:f54          68:21:5F:FB:0F:54   vlan1001        Reachable   never      Local      N/A
------------------------------------------------------------------------------------------------------------------------

Total: 6          Dynamic:1          Static:1
```

10.1.3 Application cases

N/A

11 IPv6 Routing Configuration

11.1 Configuring IPv6 Unicast-Routing

11.1.1 Overview

Function Introduction

Static routing is a special type of routing that is manually configured by an administrator.When the network structure is relatively simple, the configuration of static routing can make the network work normally.Proper configuration and use of static routing can improve network performance and ensure bandwidth for important network applications.

The disadvantage of static routing is that when the network fails or the topology changes, the route may not be reachable, resulting in network outage.It is up to the network administrator to manually modify the configuration of the static route.

Static routing consists of a network prefix (host address) and the next hop (gateway).Static routing is useful in small networks.Static routing provides a simple solution that makes several destinations accessible.

Dynamic routing protocols are recommended for large networks.

Principle Description

N/A

11.1.2 Configuration

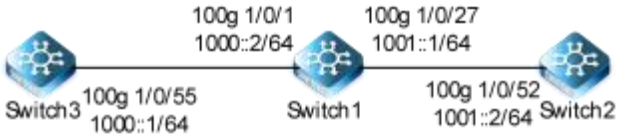


Figure 11-1 ipv6 unicast routing

The following example shows how to deploy static routes in a simple environment.

The following configuration should be operated on all switches if the switch ID is not specified.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interface configure mode and set the attributes of the interface

Configuration for Switch3:

```
switch3(config)#vlan 1000
switch3(config-100ge1/0/55)#port link-type trunk
switch3(config-100ge1/0/55)#port trunk allow-pass vlan
1000 switch3(config-100ge1/0/55)#int vlan 1000
switch3(config-vlanif-1000)#ipv6 enable
switch3(config-vlanif-1000)#ipv6 address 1000::1/64
```

```
switch3(config-vlanif-1000)#quit
```

Configuration for Switch1:

```
switch1(config)#vlan 1000-1001
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#port link-ty trunk
switch1(config-100ge1/0/31)#port trunk allow-pass vlan 1000
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port trunk allow-pass vlan 1001

switch1(config-100ge1/0/27)#int vlan 1000
switch1(config-vlanif-1000)#ipv6 enable
switch1(config-vlanif-1000)#ipv6 address 1000::2/64
switch1(config-vlanif-1000)#quit
switch1(config)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 enable
switch1(config-vlanif-1001)#ipv6 address 1001::1/64
switch1(config-vlanif-1001)#quit
```

Configuration for Switch2:

```
switch2(config)#vlan 1001
switch2(vlan-1001)#int 100g 1/0/52
switch2(config-100ge1/0/52)#port link-type trunk
switch2(config-100ge1/0/52)#port trunk allow-pass vlan 1001
switch2(config-100ge1/0/52)#int vlan 1001
switch2(config-vlanif-1001)#ipv6 enable
switch2(config-vlanif-1001)#ipv6 address 1001::2/64
switch2(config-vlanif-1001)#quit
```

step 3 Configure static routes

Configuring Switch2:

```
switch2(config)#ipv6 route-static 1000:: 64 1001::1
```

Configuring Switch3:

```
switch3(config)#ipv6 route-static 1001:: 64 1000::2
```

step 4 Exit the configure mode

```
switch(config)# end
```

step 5 Validation

Display the result on Switch3:

```
switch3(config)#show ipv6 route

  Routing Tables: Public
  Dest/Prefixlen                          Nexthop                    Interface          Proto     Cost
  ------------------------------------------------------------------------------------------------------
  ::1/128                                 ::1                        loopback0          local     1
  1000::/64                               1000::1                    vlan1000           local     1
  1000::1/128                             1000::1                    vlan1000           local     1
  1001::/64                               1001::2                    vlan1001           local     1
  1001::/64                               1000::2                    vlan1000           static    60
  1001::2/128                             1001::2                    vlan1001           local     1
  fe80::/64                               fe80::6a50:ff:fedb:fc00    loopback0          local     1
  fe80::6a50:ff:fedb:fc00/128             fe80::6a50:ff:fedb:fc00    loopback0          local     1
  fe80::/64                               fe80::6a21:5fff:fedb:fc00  vlan1000          local     1
  fe80::6a21:5fff:fedb:fc00/128           fe80::6a21:5fff:fedb:fc00  vlan1000          local     1
  fe80::/64                               fe80::6a21:5fff:fedb:fc00  vlan1001          local     1
  fe80::6a21:5fff:fedb:fc00/128           fe80::6a21:5fff:fedb:fc00  vlan1001          local     1
  fe80::/64                               fe80::6a50:1ff:fedb:fc00   loopback1         local     1
  fe80::6a50:1ff:fedb:fc00/128            fe80::6a50:1ff:fedb:fc00   loopback1         local     1
  ------------------------------------------------------------------------------------------------------
  Total: 14                Static: 1
```

Display the result on Switch2:

```
switch2(config)#show ipv6 route

  Routing Tables: Public
  Dest/Prefixlen                          Nexthop                    Interface          Proto     Cost
  ------------------------------------------------------------------------------------------------------
  ::1/128                                 ::1                        loopback0          local     1
  1000::/64                               1001::1                    vlan1001           static    60
  1001::/64                               1001::2                    vlan1001           local     1
  1001::2/128                             1001::2                    vlan1001           local     1
  1003::/64                               1003::1                    vlan1003           local     1
  1003::1/128                             1003::1                    vlan1003           local     1
  1212::/64                               1212::3                    loopback1          local     1
  1212::3/128                             1212::3                    loopback1          local     1
  2202::/64                               2202::2                    loopback2          local     1
  2202::2/128                             2202::2                    loopback2          local     1
  fe80::/64                               fe80::6a50:ff:feb7:5b10    loopback0          local     1
  fe80::6a50:ff:feb7:5b10/128             fe80::6a50:ff:feb7:5b10    loopback0          local     1
  fe80::/64                               fe80::6a21:5fff:feb7:5b10  vlan1001          local     1
  fe80::6a21:5fff:feb7:5b10/128           fe80::6a21:5fff:feb7:5b10  vlan1001          local     1
  fe80::/64                               fe80::6a21:5fff:feb7:5b10  vlan1003          local     1
  fe80::6a21:5fff:feb7:5b10/128           fe80::6a21:5fff:feb7:5b10  vlan1003          local     1
  fe80::/64                               fe80::6a50:1ff:feb7:5b10   loopback1         local     1
  fe80::6a50:1ff:feb7:5b10/128            fe80::6a50:1ff:feb7:5b10   loopback1         local     1
  fe80::/64                               fe80::6a50:2ff:feb7:5b10   loopback2         local     1
  fe80::6a50:2ff:feb7:5b10/128            fe80::6a50:2ff:feb7:5b10   loopback2         local     1
```

```
-------------------------------------------------------------------------------------------------------------
Total: 20                    Static: 1
```

Display the result on Switch3:

```
Switch# show ipv6 route
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
       [*] - [AD/Metric]
Timers: Uptime
S       2001:1::/64 [1/0]
       via 2001:2::2, eth-0-17, 00:02:14
C       2001:2::/64
       via ::, eth-0-17, 00:03:28
C       2001:2::3/128
       via ::1, eth-0-17, 00:03:28
C       fe80::/10
       via ::, Null0, 00:03:53
```

Use the "ping" command on switch2 to contact the switch3:

```
switch3(config)#ping6 1001::2

PING 1001::2: 64 data bytes
Reply from 1001::2: bytes=64 time=0ms icmp_seq=0
Reply from 1001::2: bytes=64 time=0ms icmp_seq=1
Reply from 1001::2: bytes=64 time=0ms icmp_seq=2
Reply from 1001::2: bytes=64 time=0ms icmp_seq=3
Reply from 1001::2: bytes=64 time=0ms icmp_seq=4
PING Statistics for 1001::2
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

11.1.3 Application cases

N/A

11.2 Configuring OSPFv3

11.2.1 Overview

Function Introduction

The Open Shortest Path First (OSPF) protocol is a link-state Interior Gateway Protocol (IGP) developed by the Internet Engineering Task Force (IETF).OSPF Version 3 (OSPFv3), as defined in RFC 2740 and expanded in RFC 5340, is a modification of OSPFv2 allowing IPv6 support.OSPFv3 and OSPFv2 are similar in many ways:

- Router ID,Area ID and LSA Link State ID are 32-bit.
- Hello, DD, LSR, LSU, and LSAck packets.

- Interface state machine and neighbor state machine.
- Flooding mechanism.

The following aspects of OSPFv3 and OSPFv2 are different:

- OSPFv3 runs on IPv6, which is based on links rather than network segments.
- OSPFv3 supports multi-instance on a link.
- OSPFv3 topological relations and IPv6 prefix information separation.
- OSPFv3 uses the Link-local address as the route to the next hop.
- In OSPFv3, information about the flooding scope is added in the LSA Type field.
- OSPFv3 supports two new LSAs: Link LSA and Intra Area Prefix LSA

Principle Description

The OSPFv3 module is based on the following RFC: RFC 5340 – OSPF for IPv6

11.2.2 Configuration

Basic OSPFv3 Parameters Configuration

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Create OSPFv3 instance

```
switch(config)#router ipv6 ospf
switch(config-ospfv3-1)#router-id 1.1.1.1
switch(config-ospfv3-1)#quit
```

Note： Use the command “no router ipv6 ospf process-id” in global configure mode to delete the OSPFv3 instance.

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

```
switch(config)#show ipv6 ospf confi
Version:OSPFV3_VX2.10.04.00
!
router ipv6 ospf 1
 router-id 1.1.1.1
```

Enabling OSPFv3 on an Interface

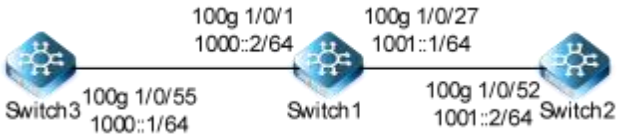


Figure 11-2 OSPFv3

Configure basic OSPFv3 functions on switch1-3 to ensure that devices on the network can communicate with each other.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Configure an IPv6 address for each interface

 # Configure Switch 3.

```
switch3(config)#vlan 1000
switch3(config-100ge1/0/55)#port link-type trunk
switch3(config-100ge1/0/55)#port trunk allow-pass vlan 1000
switch3(config-100ge1/0/55)#int vlan 1000
switch3(config-vlanif-1000)#ipv6 enable
switch3(config-vlanif-1000)#ipv6 address 1000::1/64
switch3(config-vlanif-1000)#quit
```

 # Configure Switch 1.

```
switch1(config)#vlan 1000-1001
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#port link-ty trunk
switch1(config-100ge1/0/31)#port trunk allow-pass vlan 1000
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port trunk allow-pass vlan 1001

switch1(config-100ge1/0/27)#int vlan 1000
switch1(config-vlanif-1000)#ipv6 enable
switch1(config-vlanif-1000)#ipv6 address 1000::2/64
switch1(config-vlanif-1000)#quit
switch1(config)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 enable
switch1(config-vlanif-1001)#ipv6 address 1001::1/64
switch1(config-vlanif-1001)#quit
```

 # Configure Switch 2.

```
switch2(config)#vlan 1001
switch2(vlan-1001)#int 100g 1/0/52
switch2(config-100ge1/0/52)#port link-type trunk
```

```
switch2(config-100ge1/0/52)#port trunk allow-pass vlan 1001
switch2(config-100ge1/0/52)#int vlan 1001
switch2(config-vlanif-1001)#ipv6 enable
switch2(config-vlanif-1001)#ipv6 address 1001::2/64
switch2(config-vlanif-1001)#quit
```

step 3 Create OSPFv3 instance

 # Configure Switch 3.

```
switch3(config)#router ipv6 ospf
switch3(config-ospfv3-1)#router-id 1.1.1.1
switch3(config-ospfv3-1)#quit
```

 # Configure Switch 1.

```
switch1(config)#router ipv6 ospf
switch1(config-ospfv3-1)#router-id 2.2.2.2
switch1(config-ospfv3-1)#quit
```

 # Configure Switch 2.

```
switch2(config)#router ipv6 ospf
switch2(config-ospfv3-1)#router-id 3.3.3.3
switch2(config-ospfv3-1)#quit
```

step 4 Enter the interface to configure OSPFv3

 # Configure Switch 3.

```
switch3(config)#int vlan 1000
switch3(config-vlanif-1000)#ipv6 ospf area 0 process 1
```

 # Configure Switch 1.

```
switch1(config)#int vlan 1000
switch1(config-vlanif-1000)#ipv6 ospf area 0
switch1(config-vlanif-1000)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 ospf area 1
switch1(config-vlanif-1001)#quit
```

 # Configure Switch 2.

```
switch2(config)#int vlan 1001
switch2(config-vlanif-1001)#ipv6 ospf area 1
switch2(config-vlanif-1001)#quit
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

#Display switch 3.

```
switch3(config)#show ipv6 ospf neighbor

 Ospfv3 Process 1
 NeighborId          Priority  State       Interface       Instance  Aging      UpTime     IpAddress
 2.2.2.2             1         Full        vlan1000        0         39         0:03:26    fe80::6a21:5fff:fefb:f54

switch3(config)#show ipv6 ospf database
 Database of OSPFv3 Process 1


                 Router Link State (Area 0.0.0.0)
 LinkId              ADV Router          Age       Seq#          CheckSum     Len
 0.0.0.0             1.1.1.1             234       0x80000002    0xb528       40
 0.0.0.0             2.2.2.2             232       0x80000003    0x983f       40

                 Network Link State (Area 0.0.0.0)
 LinkId              ADV Router          Age       Seq#          CheckSum     Len
0.0.51.232           1.1.1.1             235       0x80000001    0x4cb0       32

                 Inter Area Prefix Link State (Area 0.0.0.0)
 LinkId              ADV Router          Age       Seq#          CheckSum     Len       Prefix
 0.0.0.2             2.2.2.2             230       0x80000001    0x6d1        36        1001::/64

                 Intra Area Prefix Link State (Area 0.0.0.0)
 LinkId              ADV Router          Age       Seq#          CheckSum     Len
 0.0.3.232           1.1.1.1             235       0x80000001    0xd8cc       44

                 Link(Type-8) State(interface vlan1000 Area 0.0.0.0)
 LinkId              ADV Router          Age       Seq#          CheckSum     Len
 0.0.51.232          1.1.1.1             423       0x80000001    0xe7e5       76
 0.0.51.232          2.2.2.2             275       0x80000001    0x4101       76

switch3(config)#show ipv6 ospf route

 Ospfv3 Process 1
 RoutType  Prefix                AreaId      PathType    Cost     Cost2       NextHopIf    NextHopNbr
BackupNextHop
 ABR       2.2.2.2/128           0.0.0.0     INTRA       1        0           64           fe80::6a21:5fff:fefb:f54        ::
 PREFIX    1000::/64             0.0.0.0     INTRA       1        0           64           ::                              ::
 PREFIX    1001::/64             0.0.0.0     INTER       2        0           64           fe80::6a21:5fff:fefb:f54        ::
```

#Display switch 1.

```
switch1(config)#show ipv6 ospf neighbor

 Ospfv3 Process 1
 NeighborId          Priority  State       Interface       Instance  Aging      UpTime     IpAddress
```

```
1.1.1.1          1       Full    vlan1000        0       30      0:05:02   fe80::6a21:5fff:fedb:fc00
3.3.3.3          1       Full    vlan1001        0       30      0:03:36   fe80::6a21:5fff:feb7:5b10

switch1(config)#show ipv6  ospf database
 Database of OSPFv3 Process 1



                Router Link State (Area 0.0.0.0)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len
 0.0.0.0         1.1.1.1         317         0x80000002 0xb528    40
 0.0.0.0         2.2.2.2         314         0x80000003 0x983f    40

                Network Link State (Area 0.0.0.0)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len
0.0.51.232       1.1.1.1         318         0x80000001 0x4cb0    32

               Inter Area Prefix Link State (Area 0.0.0.0)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len  Prefix
 0.0.0.2         2.2.2.2         312         0x80000001 0x6d1     36   1001::/64

               Intra Area Prefix Link State (Area 0.0.0.0)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len
 0.0.3.232       1.1.1.1         317         0x80000001 0xd8cc    44

               Link(Type-8) State(interface vlan1000 Area 0.0.0.0)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len
 0.0.51.232      1.1.1.1         506         0x80000001 0xe7e5    76
 0.0.51.232      2.2.2.2         356         0x80000001 0x4101    76

                Router Link State (Area 0.0.0.1)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len
 0.0.0.0         2.2.2.2         231         0x80000002 0xdc5     40
 0.0.0.0         3.3.3.3         232         0x80000002 0xebe3    40

                Network Link State (Area 0.0.0.1)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len
0.0.51.233       2.2.2.2         231         0x80000001 0x7877    32

               Inter Area Prefix Link State (Area 0.0.0.1)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len  Prefix
 0.0.0.2         2.2.2.2         313         0x80000001 0xf9de    36   1000::/64

               Intra Area Prefix Link State (Area 0.0.0.1)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len
 0.0.3.232       2.2.2.2         231         0x80000001 0xb90     44

               Link(Type-8) State(interface vlan1001 Area 0.0.0.1)
 LinkId          ADV Router      Age         Seq#       CheckSum  Len
```

```
0.0.51.233      2.2.2.2      313      0x80000001   0x49f6   76
0.0.51.233      3.3.3.3      272      0x80000001   0x7403   76

switch1(config)#show ipv6 ospf route

 Ospfv3 Process 1
 RoutType   Prefix              AreaId      PathType   Cost   Cost2   NextHopIf   NextHopNbr
BackupNextHop
 PREFIX     1000::/64           0.0.0.0     INTRA      1      0
940         ::                             ::
 PREFIX     1001::/64           0.0.0.1     INTRA      1      0
941         ::                             ::
```

Configuring OSPFv3 Stub Areas

Figure 11-3 OSPFv3 areas

You can optionally configure multiple OSPFv3 region parameters.These parameters configure the region as a Stub.A stub area is a special area where the ABRs do not flood the received external routes. In stub areas, the size of the routing table of the routers and the routing information in transmission are reduced.To ensure the reachability of a destination outside the AS, the ABR in the stub area generates a default route and advertises it to the non-ABR routers in the stub area.

The following configuration should be operated on all switches if the switch ID is not specified.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface to configure interface properties

 # Configure Switch 3.

```
switch3(config)#vlan 1000
switch3(config-100ge1/0/55)#port link-type trunk
switch3(config-100ge1/0/55)#port trunk allow-pass vlan 1000
switch3(config-100ge1/0/55)#int vlan 1000
switch3(config-vlanif-1000)#ipv6 enable
switch3(config-vlanif-1000)#ipv6 address 1000::1/64
switch3(config-vlanif-1000)#quit
```

 # Configure Switch 1.

```
switch1(config)#vlan 1000-1001
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#port link-ty trunk
switch1(config-100ge1/0/31)#port trunk allow-pass vlan 1000
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port trunk allow-pass vlan 1001

switch1(config-100ge1/0/27)#int vlan 1000
switch1(config-vlanif-1000)#ipv6 enable
switch1(config-vlanif-1000)#ipv6 address 1000::2/64
switch1(config-vlanif-1000)#quit
switch1(config)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 enable
switch1(config-vlanif-1001)#ipv6 address 1001::1/64
switch1(config-vlanif-1001)#quit
```

 # Configure Switch 2.

```
switch2(config)#vlan 1001
switch2(vlan-1001)#int 100g 1/0/52
switch2(config-100ge1/0/52)#port link-type trunk
switch2(config-100ge1/0/52)#port trunk allow-pass vlan 1001
switch2(config-100ge1/0/52)#int vlan 1001
switch2(config-vlanif-1001)#ipv6 enable
switch2(config-vlanif-1001)#ipv6 address 1001::2/64
switch2(config-vlanif-1001)#quit
```

step 3 Create OSPFv3 instance

 # Configure Switch 3.

```
switch3(config)#router ipv6 ospf
switch3(config-ospfv3-1)#router-id 1.1.1.1
switch3(config-ospfv3-1)#quit
```

 # Configure Switch 1.

```
switch1(config)#router ipv6 ospf
switch1(config-ospfv3-1)#router-id 2.2.2.2
switch1(config-ospfv3-1)#area 1 stub
switch1(config-ospfv3-1)#quit
```

 # Configure Switch 2.

```
switch2(config)#router ipv6 ospf
switch2(config-ospfv3-1)#router-id 3.3.3.3
switch2(config-ospfv3-1)#area 1 stub
switch2(config-ospfv3-1)#quit
```

step 4 Enter the interface configure OSPFv3

 # Configure Switch 3.

```
switch3(config)#int vlan 1000
switch3(config-vlanif-1000)#ipv6 ospf area 0 process 1
```

 # Configure Switch 1.

```
switch1(config)#int vlan 1000
switch1(config-vlanif-1000)#ipv6 ospf area 0
switch1(config-vlanif-1000)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 ospf area 1
switch1(config-vlanif-1001)#quit
```

 # Configure Switch 2.

```
switch2(config)#int vlan 1001
switch2(config-vlanif-1001)#ipv6 ospf area 1
switch2(config-vlanif-1001)#quit
```

Step 5 OSPFv3 Stub Areas introduces external routes

#Configure BGP external route. Router BGP 101 is configured as below:

```
switch2(config)#vlan 1002
switch2(vlan-1002)#int 10g 1/0/58
switch2(config-10ge1/0/58)#port hybrid vlan 1002 tagged
switch2(config-10ge1/0/58)#quit
switch2(config)#int vlan 1002
switch2(config-vlanif-1002)#ipv6 enable
switch2(config-vlanif-1002)#ipv6 address 1002::1/64
switch2(config-vlanif-1002)#quit

switch2(config)#router bgp 100
switch2(config-bgp)#neighbor 1002::2 remote-as 101
switch2(config-bgp)#quit
```

#ospfv3 introduces external route.

```
switch2(config)#router ipv6 ospf
switch2(config-ospfv3-1)#redistribute bgp
```

Step 6 Exit the configure mode

```
Switch(config)# end
```

Step 7 Validation

#Display switch 3.

```
switch3#show ipv6 route
  Routing Tables: Public
  Dest/Prefixlen                          Nexthop                    Interface          Proto     Cost
  ------------------------------------------------------------------------------------------------------------------------------------------
  ::1/128                                 ::1                        loopback0          local     1
  1000::/64                               1000::1                    vlan1000           local     1
  1000::1/128                             1000::1                    vlan1000           local     1
  1001::/64                               fe80::6a21:5fff:fefb:f54   vlan1000           ospf      1
  fe80::/64                               fe80::6a50:ff:fedb:fc00    loopback0          local     1
  fe80::6a50:ff:fedb:fc00/128             fe80::6a50:ff:fedb:fc00    loopback0          local     1
  fe80::/64                               fe80::6a21:5fff:fedb:fc00  vlan1000           local     1
  fe80::6a21:5fff:fedb:fc00/128           fe80::6a21:5fff:fedb:fc00  vlan1000           local     1
  fe80::/64                               fe80::6a50:1ff:fedb:fc00   loopback1          local     1
  fe80::6a50:1ff:fedb:fc00/128            fe80::6a50:1ff:fedb:fc00   loopback1          local     1
  ------------------------------------------------------------------------------------------------------------------------------------------
  Total: 10                Static: 0
```

#Display switch 1.

```
switch1#show ipv6 route
  Routing Tables: Public
  Dest/Prefixlen                          Nexthop                    Interface          Proto     Cost
  ------------------------------------------------------------------------------------------------------------------------------------------
  ::1/128                                 ::1                        loopback0          local     1
  112::/64                                112::3                     loopback2          local     1
  112::3/128                              112::3                     loopback2          local     1
  1000::/64                               1000::2                    vlan1000           local     1
  1000::2/128                             1000::2                    vlan1000           local     1
  1001::/64                               1001::1                    vlan1001           local     1
  1001::1/128                             1001::1                    vlan1001           local     1
  fe80::/64                               fe80::6a50:ff:fefb:f54     loopback0          local     1
  fe80::6a50:ff:fefb:f54/128              fe80::6a50:ff:fefb:f54     loopback0          local     1
  fe80::/64                               fe80::6a21:5fff:fefb:f54   vlan1000           local     1
  fe80::6a21:5fff:fefb:f54/128            fe80::6a21:5fff:fefb:f54   vlan1000           local     1
  fe80::/64                               fe80::6a21:5fff:fefb:f54   vlan1001           local     1
  fe80::6a21:5fff:fefb:f54/128            fe80::6a21:5fff:fefb:f54   vlan1001           local     1
  fe80::/64                               fe80::6a50:2ff:fefb:f54    loopback2          local     1
  fe80::6a50:2ff:fefb:f54/128             fe80::6a50:2ff:fefb:f54    loopback2          local     1
  ------------------------------------------------------------------------------------------------------------------------------------------
  Total: 15                Static: 0
```

#Display switch 2.

```
switch2(config)#show ipv6 route
  Routing Tables: Public
```

Dest/Prefixlen	Nexthop	Interface	Proto	Cost
::/0	fe80::6a21:5fff:fefb:f54	vlan1001	ospf	1
::1/128	::1	loopback0	local	1
1000::/64	fe80::6a21:5fff:fefb:f54	vlan1001	ospf	1
1001::/64	1001::2	vlan1001	local	1
1001::2/128	1001::2	vlan1001	local	1
1002::/64	1002::1	vlan1002	local	1
1002::1/128	1002::1	vlan1002	local	1
1003::/64	1003::1	vlan1003	local	1
1003::1/128	1003::1	vlan1003	local	1
1212::/64	1212::3	loopback1	local	1
1212::3/128	1212::3	loopback1	local	1
2001:1:1::/64	1002::2	vlan1002	bgp	1
2001:1:1:1::/64	1002::2	vlan1002	bgp	1
2001:1:1:2::/64	1002::2	vlan1002	bgp	1
2001:1:1:3::/64	1002::2	vlan1002	bgp	1
2001:1:1:4::/64	1002::2	vlan1002	bgp	1
2202::/64	2202::2	loopback2	local	1
2202::2/128	2202::2	loopback2	local	1
fe80::/64	fe80::6a50:ff:feb7:5b10	loopback0	local	1
fe80::6a50:ff:feb7:5b10/128	fe80::6a50:ff:feb7:5b10	loopback0	local	1
fe80::/64	fe80::6a21:5fff:feb7:5b10	vlan1001	local	1
fe80::6a21:5fff:feb7:5b10/128	fe80::6a21:5fff:feb7:5b10	vlan1001	local	1
fe80::/64	fe80::6a21:5fff:feb7:5b10	vlan1002	local	1
fe80::6a21:5fff:feb7:5b10/128	fe80::6a21:5fff:feb7:5b10	vlan1002	local	1
fe80::/64	fe80::6a21:5fff:feb7:5b10	vlan1003	local	1
fe80::6a21:5fff:feb7:5b10/128	fe80::6a21:5fff:feb7:5b10	vlan1003	local	1
fe80::/64	fe80::6a50:1ff:feb7:5b10	loopback1	local	1
fe80::6a50:1ff:feb7:5b10/128	fe80::6a50:1ff:feb7:5b10	loopback1	local	1
fe80::/64	fe80::6a50:2ff:feb7:5b10	loopback2	local	1
fe80::6a50:2ff:feb7:5b10/128	fe80::6a50:2ff:feb7:5b10	loopback2	local	1

Total: 30 Static: 0

Configuring OSPFv3 NSSA Areas

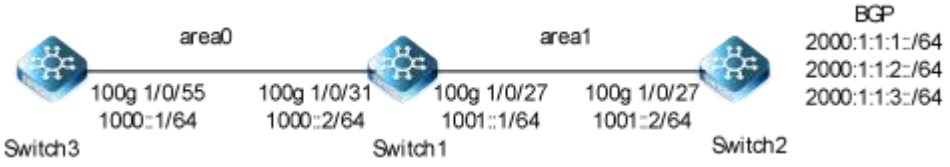


Figure 11-4 OSPFv3 area

An excessive number of entries in a routing table cause high CPU usage. To reduce the number of entries in a routing table, configure a non-backbone area on the border of an AS as a stub area or an NSSA to reduce the amount of routing information to be transmitted.

OSPFv3 stub areas cannot import or transmit external routes. If you need to import external routes to an area and prevent these routes from consuming resources, configure the area as an NSSA. NSSAs can import AS external routes and advertise them within the entire AS, without learning external routes from other areas in the AS, which reduces bandwidth and storage resource consumption on the device.

An NSSA requires NSSA attributes on all the devices in this area.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface to configure interface properties

 # Configure Switch 3.

```
switch3(config)#vlan 1001
switch3(config)#int 100g 1/0/55
switch3(config-100ge1/0/55)#port hybrid vlan 1001 tagged
switch3(config-100ge1/0/55)#int vlan 1001
switch3(config-vlanif-1001)#ipv6 enable
switch3(config-vlanif-1001)#ipv6   address 1001::1/64
switch3(config-vlanif-1001)#quit
```

 # Configure Switch 1.

```
switch1(config)#vlan 1000-1001
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#port hybrid vlan 1001 tagged
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port hybrid vlan 1002 tagged
switch1(config-100ge1/0/27)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 address 1001::2/24
switch1(config-vlanif-1001)#int vlan 1002
switch1(config-vlanif-1002)#ipv6 address 1002::1/64
```

 # Configure Switch 2.

```
switch2(config)#vlan 1002
switch2(vlan-1001)#int 100g 1/0/52
switch2(config-100ge1/0/52)#port hybrid vlan 1002
tagged switch2(config-100ge1/0/52)#int vlan 1002
switch2(config-vlanif-1001)#ipv6 enable
switch2(config-vlanif-1001)#ipv6 address 1002::2/64
switch2(config-vlanif-1001)#quit
```

step 3 Create OSPFv3 instance

 # Configure Switch 3.

```
switch3(config)#router ipv6 ospf
switch3(config-ospfv3-1)#quit
```

 # Configure Switch 1.

```
switch1(config)#router ipv6 ospf
switch1(config-ospfv3-1)#area 1 nssa
switch1(config-ospfv3-1)#quit
```

 # Configure Switch 2.

```
switch2(config)#router ipv6 ospf
switch2(config-ospfv3-1)#router-id 3.3.3.3
switch2(config-ospfv3-1)#area 1 nssa
switch2(config-ospfv3-1)#quit
```

step 4 Enter the interface configure OSPFv3

 # Configure Switch 3.

```
switch3(config)#int vlan 1001
switch3(config-vlanif-1001)#ipv6 ospf area 0 process 1
```

 # Configure Switch 1.

```
switch1(config)#int vlan 1001
switch1(config-vlanif-1001)#ipv6 ospf area 0
switch1(config-vlanif-1001)#int vlan 1002
switch1(config-vlanif-1002)#ipv6 ospf area 1
switch1(config-vlanif-1001)#quit
```

 # Configure Switch 2.

```
switch2(config)#int vlan 1002
switch2(config-vlanif-1002)#ipv6 ospf area 1
switch2(config-vlanif-1002)#quit
```

Step 5 OSPFv3 NSSA Areas introduces external routes

#Configure BGP external route. Router BGP 101 is configured as below:

```
switch2(config)#vlan 1003
switch2(vlan-1002)#int 10g 1/0/58
switch2(config-10ge1/0/58)#port hybrid vlan 1003 tagged
switch2(config-10ge1/0/58)#quit
switch2(config)#int vlan 1003
switch2(config-vlanif-1003)#ipv6 enable
switch2(config-vlanif-1003)#ipv6 address 1003::1/64
```

```
switch2(config-vlanif-1003)#quit

switch2(config)#router bgp 100
switch2(config-bgp)#neighbor 1003::2 remote-as 101
switch2(config-bgp)#quit
```

#ospfv3 introduces external route.

```
switch2(config)#router ipv6 ospf
switch2(config-ospfv3-1)#redistribute bgp
switch2(config-ospfv3-1)#redistribute connect
```

Step 6 Exit the configure mode

```
Switch(config)# end
```

step 7 Validation

#Display switch 3.

```
switch3(config)#show ipv ospf route

 Ospfv3 Process 1
 RoutType  Prefix                AreaId      PathType    Cost    Cost2    NextHopIf   NextHopNbr
BackupNextHop
 ABR       112.133.32.10/128     0.0.0.0     INTRA       1       0        63          fe80::6a21:5fff:fefb:f54   ::
 ASBR      112.133.32.10/128     0.0.0.0     INTRA       1       0        63          fe80::6a21:5fff:fefb:f54   ::
 ASBR      113.133.32.10/128     0.0.0.0     INTER       2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    44:0:0:1::/64         0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    44:0:0:2::/64         0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    44:0:0:3::/64         0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    44:0:0:4::/64         0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    44:0:0:5::/64         0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    1001::/24             0.0.0.0     INTRA       1       0
63         ::                                ::
 PREFIX    1001::/64             0.0.0.0     INTRA       1       0
63         ::                                ::
 PREFIX    1002::/64             0.0.0.0     INTER       2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    1002::2/128           0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    1003::/64             0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    1003::1/128           0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    1005::/64             0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    1005::1/128           0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    1100::/64             0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
 PREFIX    1100::2/128           0.0.0.0     EXTERNAL_1  2       0        63          fe80::6a21:5fff:fefb:f54   ::
```

#Display switch 1.

```
switch1(config)#show ipv6 ospf route

 Ospfv3 Process 1
 RoutType  Prefix                  AreaId      PathType   Cost   Cost2   NextHopIf  NextHopNbr
BackupNextHop
 ASBR      114.133.32.10/128       0.0.0.0     INTRA      1      0       443        fe80::6a21:5fff:fedb:fc00      ::
 ASBR      113.133.32.10/128       0.0.0.1     INTRA      1      0       38
fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    44:0:0:1::/64           0.0.0.0     EXTERNAL_1 2      0       38         fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    44:0:0:2::/64           0.0.0.0     EXTERNAL_1 2      0       38         fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    44:0:0:3::/64           0.0.0.0     EXTERNAL_1 2      0       38         fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    44:0:0:4::/64           0.0.0.0     EXTERNAL_1 2      0       38         fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    44:0:0:5::/64           0.0.0.0     EXTERNAL_1 2      0       38         fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    1000::/64               0.0.0.0     EXTERNAL_1 2      0       443        fe80::6a21:5fff:fedb:fc00      ::
 PREFIX    1000::2/128             0.0.0.0     EXTERNAL_1 2      0       443        fe80::6a21:5fff:fedb:fc00      ::
 PREFIX    1001::/24               0.0.0.0     INTRA      1      0
443        ::                                  ::
 PREFIX    1001::/64               0.0.0.0     INTRA      1      0
443        ::                                  ::
 PREFIX    1001::1/128             0.0.0.0     EXTERNAL_1 2      0       443        fe80::6a21:5fff:fedb:fc00      ::
 PREFIX    1002::/64               0.0.0.1     INTRA      1      0
38         ::                                  ::
 PREFIX    1002::2/128             0.0.0.0     EXTERNAL_1 2      0       38
fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    1003::/64               0.0.0.0     EXTERNAL_1 2      0       38
fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    1003::1/128             0.0.0.0     EXTERNAL_1 2      0       38
fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    1005::/64               0.0.0.0     EXTERNAL_1 2      0       38
fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    1005::1/128             0.0.0.0     EXTERNAL_1 2      0       38
fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    1100::/64               0.0.0.0     EXTERNAL_1 2      0       38
fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    1100::2/128             0.0.0.0     EXTERNAL_1 2      0       38
fe80::6a21:5fff:feb7:5b10      ::
 PREFIX    8800:0:0:1::/64         0.0.0.0     EXTERNAL_1 2      0       443        fe80::6a21:5fff:fedb:fc00      ::
 PREFIX    8800:0:0:2::/64         0.0.0.0     EXTERNAL_1 2      0       443        fe80::6a21:5fff:fedb:fc00      ::
 PREFIX    8800:0:0:3::/64         0.0.0.0     EXTERNAL_1 2      0       443        fe80::6a21:5fff:fedb:fc00      ::
 PREFIX    8800:0:0:4::/64         0.0.0.0     EXTERNAL_1 2      0       443        fe80::6a21:5fff:fedb:fc00      ::
 PREFIX    8800:0:0:5::/64         0.0.0.0     EXTERNAL_1 2      0       443        fe80::6a21:5fff:fedb:fc00      ::
```

#Display switch 2.

```
switch2(config)#show ipv6 ospf route

 Ospfv3 Process 1
```

RoutType	Prefix	AreaId	PathType	Cost	Cost2	NextHopIf	NextHopNbr	BackupNextHop
ABR	112.133.32.10/128	0.0.0.1	INTRA	1	0	62	fe80::6a21:5fff:fefb:f54	::
ASBR	112.133.32.10/128	0.0.0.1	INTRA	1	0	62	fe80::6a21:5fff:fefb:f54	::
PREFIX	::/0	0.0.0.0	EXTERNAL_1	1	0	62	fe80::6a21:5fff:fefb:f54	::
PREFIX	1001::/24	0.0.0.1	INTER	2	0	62	fe80::6a21:5fff:fefb:f54	::
PREFIX	1001::/64	0.0.0.1	INTER	2	0	62	fe80::6a21:5fff:fefb:f54	::
PREFIX	1002::/64	0.0.0.1	INTRA	1	0			
62	::		::					

11.2.3 Application cases

N/A

11.3 Configuring Ipv6 Prefix-list

11.3.1 Overview

Function Introduction

Routing Policy is the technology for modifying route information to change traffic route. IPv6 Prefix list is a kind of route policies that used to control and modify routing information. A IPv6 prefix list is identified by list name and contains one or more ordered entries which are processed sequentially. Each entry provides a matched range for network prefix and has a unique sequence number in the list. In the matching process， switch will check entries orderly. If an entry matches conditions, this process would finish.

Principle Description

N/A

11.3.2 Configuration

Basic Configuration

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Create IPv6 Prefix list

```
switch(config)#ipv6 prefix-list test index 1 permit 1000::1/64
```

step 3 Exit the configure mode

```
Switch(config)# end
```

step 4 Validation

```
switch(config)#show ipv6 prefix-list test
```

```
ipv6 prefix-list : test
 index: 1          permit 1000::1/64
```

Configuring Route-policy

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Create IPv6 Prefix list

```
switch(config)#ipv6 prefix-list test index 1 permit 1000::1/64
```

Step 3 Create route-policy and apply IPv6 Prefix list

```
switch(config)#route-policy p1 deny node 10
switch(config-route-policy)#match ipv6 address prefix-list test
switch(config-route-policy)#apply cost 200
switch(config-route-policy)#quit
```

step 4 Apply route-policy in OSPFv3

```
switch(config)#router ospf
switch(config-ospf-1)#redistribute static route-policy p1
switch(config-ospf-1)#quit
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Validation

```
Switch # show route-map
!
ipv6 prefix-list test index 1 permit 1000::1/64
!
route-policy p1 deny node 10
 match ipv6 address prefix-list test
 apply cost 200
!
router ospf 1
 router-id 1.1.1.1
 network 100.1.1.0 255.255.255.0 area 0
 redistribute static route-policy p1
!
router ipv6 ospf 1
```

```
router-id 1.1.1.1
```

11.3.3 Application cases

N/A

12 Vxlan Configuration Guide

12.1 Vxlan Basic Concept

12.1.1 Overview

Function Introduction

VXLAN is a network virtualization technology in NVO3, which encapsulates the packet sent by the virtual machine in UDP, USES the IP of the physical network and MAC as the outerheader for encapsulation, and then transmits the data on the IP network, after arriving at the destination, it is unsealed by the tunnel terminal and sends the data to the target virtual machine.

Principle Description

Refer ence RFC 7348.

12.1.2 VXLAN Gateway Application

VXLAN Gateway Application

Centralized VXLAN Gateway deployment： Centralized gateway means that the three-layer gateway is centrally deployed on a single device, and all traffic across the subnet is forwarded through the three-layer gateway to achieve the centralized management of traffic.

Distributed VXLAN Gateway deployment ： The disadvantages of centralized gateway deployment can be addressed by deploying distributed gateways.VXLAN distributed gateway refers to that under a typical "Spin-Leaf" network structure, Leaf nodes are used as VTEP at the end of VXLAN tunnel, and each Leaf node can be used as a three-layer gateway of VXLAN. The Spine nodes do not perceive VXLAN tunnel, but only act as the forwarding node of VXLAN message.

12.2 Configuration

12.2.1 Static Centralized VXLAN Gateway Configuration

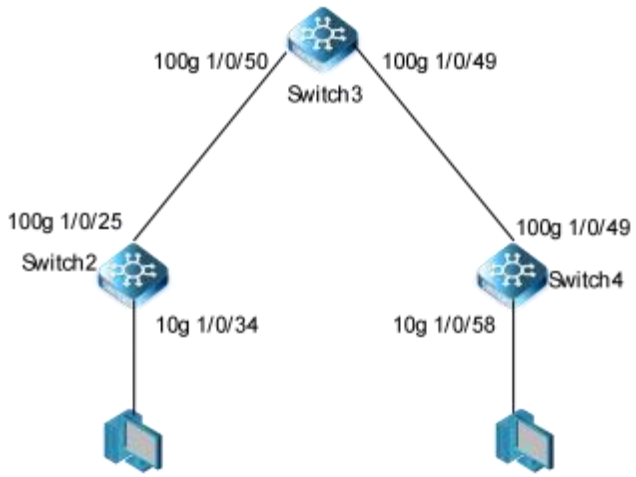


Figure 12-1 Static Centralized VXLAN Gateway

The following configurations are same on Switch2 ,Switch3 and Switch4：

step 1 Enter the configure mode

```
switch#configure
```

step 2 Create vlans

Switch2

```
sw2(config)#vlan 3000
sw2(vlan-3000)#quit
```

Switch3

```
sw3(config)#vlan 3000-3001
```

Switch4

```
sw4(config)#vlan 3001-3002
sw2(vlan-3000)#quit
```

step 3 Enter the interfaceconfigure mode and configure interface properties

Interface configuration for Switch2

```
sw2(config)#int 100g 1/0/25
sw2(config-100ge1/0/25)#port hybrid vlan 3000 tagged
sw2(config-100ge1/0/25)#exit
```

Interface configuration for Switch3

```
sw3(config)#int 100g 1/0/50
sw3(config-100ge1/0/50)#port hybrid vlan 3000 tagged
sw3(config-100ge1/0/50)#exit
sw3(config)#int 100g 1/0/49
sw3(config-100ge1/0/49)#port hybrid vlan 3001 tagged
sw3(config-100ge1/0/49)#exit
```

Interface configuration for Switch4

```
sw4(config)#interface 100gigaethernet 1/0/49
sw4(config-100ge1/0/49)#port hybrid vlan 3001 tagged
sw4(config-100ge1/0/49)#exit
```

step 4 Configure switch2,switch3 and switch4 communicate at layer through ospf

Switch2

```
sw2(config)#int loopback 1
sw2(config-loopback-1)# ip address 2.2.2.2/24
sw2(config-loopback-1)#int vlan 3000
sw2(config-vlanif-3000)#ip add 103.1.1.1/24
sw2(config-vlanif-3000)#exit
```

```
sw2(config)#router ospf
sw2(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 0
sw2(config-ospf-1)#network 103.1.1.0 255.255.255.0 area 0
sw2(config-ospf-1)#exit
```

Switch3

```
sw3(config)#int loopback 1
sw3(config-loopback-1)# ip address 3.3.3.3/24
sw3(config-loopback-1)#int vlan 3000
sw3(config-vlanif-3000)#ip add 103.1.1.2/24
sw3(config-vlanif-3000)#int vlan 3001
sw3(config-vlanif-3001)#ip add 103.2.1.1/24
sw2(config-vlanif-3001)#exit
sw3(config)#router ospf
sw3(config-ospf-1)#network 3.3.3.0 255.255.255.0 area 0
sw3(config-ospf-1)#network 103.1.1.0 255.255.255.0 area 0
sw3(config-ospf-1)#network 103.2.1.0 255.255.255.0 area 0
sw3(config-ospf-1)#exit
```

Switch4

```
sw4(config)#int loopback 1
sw4(config-loopback-1)# ip address 4.4.4.4/24
sw4(config-loopback-1)#int vlan 3001
sw4(config-vlanif-3001)#ip add 103.2.1.2/24
sw4(config-vlanif-3001)#exit
sw4(config)#router ospf
sw4(config-ospf-1)#network 4.4.4.0 255.255.255.0 area 0
sw4(config-ospf-1)#network 103.2.1.0 255.255.255.0 area 0
sw4(config-ospf-1)#exit
```

After OSPF is configured, the devices can use OSPF to learn the IP addresses of loopback interfaces of each other and successfully ping each other. The following example shows the command output on sw2 after it pings sw4:

```
sw2(config)#ping 4.4.4.4

 PING 4.4.4.4: 64 data bytes
 Reply from 4.4.4.4: bytes=64 time=0ms TTL=63 icmp_seq=1
 Reply from 4.4.4.4: bytes=64 time=0ms TTL=63 icmp_seq=2
 Reply from 4.4.4.4: bytes=64 time=0ms TTL=63 icmp_seq=3
 Reply from 4.4.4.4: bytes=64 time=0ms TTL=63 icmp_seq=4
 Reply from 4.4.4.4: bytes=64 time=0ms TTL=63 icmp_seq=5
 PING Statistics for 4.4.4.4
 5 packets transmitted, 5 packets received, 0% packet loss
 round-trip (ms)  min/avg/max = 0/0/0
```

step 5 Configure a service access point on sw2 and sw4

Switch2

```
sw2(config)#bridge-domain 10
sw2(config-bridge-domain-10)#vxlan vni 10
sw2(config)#int 10g 1/0/34.10
sw2(config-10ge1/0/34.10)# encapsulation untag
sw2(config-10ge1/0/34.10)# bridge-domain bind 10
sw2(config-10ge1/0/34.10)# exit
```

Switch4

```
sw4(config)#bridge-domain 10
sw4(config-bridge-domain-10)#vxlan vni 10
sw4(config)#int 10g 1/0/58.10
sw4(config-10ge1/0/58.10)# encapsulation untag
sw4(config-10ge1/0/58.10)# bridge-domain bind 10
sw2(config-10ge1/0/58.10)# exit
```

step 6 Create a VXLAN tunnel on sw2 and sw4

Switch2

```
sw2(config)#int nve 1
sw2(config-nve-1)# tunnel source 2.2.2.2
sw2(config-nve-1)# vni 10 ucast-peer 4.4.4.4
sw2(config-nve-1)# exit
```

Switch4

```
sw4(config)#int nve 1
sw4(config-nve-1)# tunnel source 4.4.4.4
sw4(config-nve-1)# vni 10 ucast-peer 2.2.2.2
sw4(config-nve-1)# exit
```

step 7 Verify the configuration

After configurating the configurations, run the **show nve peer** command on sw2,sw4 to check the VXLAN tunnel status. The follow example shows the command output on the switch2:

```
sw2(config)#show nve peer
  Interface        Vni        Peer                 State
  nve1              10        4.4.4.4               up
```

12.2.2 Centralized VXLAN Gateway Configuration in BGP EVPN mode

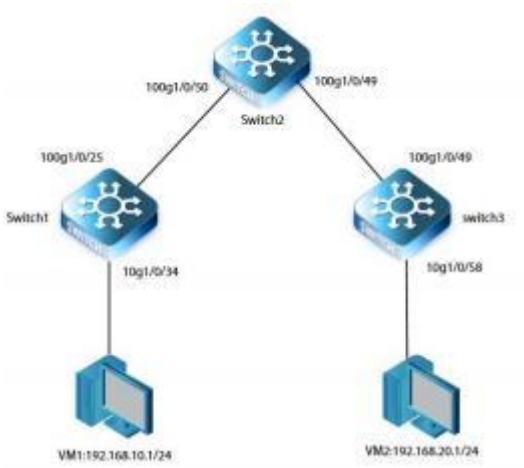


Figure 12-2 Centralized VXLAN Gateway in BGP EVPN mode

The following configurations are same on Switch1 ,Switch2 and Switch3：

step 1 Enter the configure mode

```
switch#configure
```

step 2 Create vlans

Switch1

```
Sw1(config)#vlan 10,11
Sw1(config)#
```

Switch2

```
Sw2(config)#vlan 11,12
Sw2(config)#
```

Switch3

```
Sw3(config)#vlan 12,20
Sw3(config)#
```

step 3 Enter the interfaceconfigure mode and configure interface properties

Switch1

```
Sw1(config)#int vlan 11
Sw1(config-vlanif-11)#ip address 11.0.0.1/24

Sw1(config-vlanif-11)#int 100g 1/0/25
Sw1(config-100g 1/0/25)#port hybrid vlan 11 tagged
Sw1(config-100g 1/0/25)#exit
```

```
Sw1(config)#int loopback 1
Sw1(config)#ip address 1.1.1.1/32
```

Switch2

```
Sw2(config)#int vlan 11
Sw2(config-vlanif-11)#ip address 11.0.0.2/24

Sw2(config-vlanif-11)#int 100g 1/0/50
Sw2(config-100g 1/0/50)#port hybrid vlan 11 tagged
Sw2(config-100g 1/0/50)#exit

Sw2(config)#int vlan 12
Sw2(config-vlanif-12)#ip address 12.0.0.2/24

Sw2(config-vlanif-12)#int 100g 1/0/49
Sw2(config-100g 1/0/49)#port hybrid vlan 12 tagged

Sw2(config-100g 1/0/49)#int loopback 1
Sw2(config-100g 1/0/49)#ip address 2.2.2.2/32
```

Switch3

```
Sw3(config)#int vlan 12
Sw3(config-vlanif-12)#ip address 12.0.0.1/24

Sw3(config-vlanif-12)#int 100g 1/0/49
Sw3(config-100g 1/0/49)#port hybrid vlan 12 tagged

Sw3(config-100g 1/0/49)#int loopback 1
Sw3(config-100g 1/0/49)#ip address 3.3.3.3/32
```

step 4 Configure switch1,switch2 and switch3 communicate at underlay through ospf

Switch1

```
Sw1(config)#router ospf
Sw1(config-ospf-1)#router-id 1.1.1.1
Sw1(config-ospf-1)#network 1.1.1.1 255.255.255.255 area 0
Sw1(config-ospf-1)#network 11.0.0.0 255.255.255.0 area 0
Sw1(config-ospf-1)#exit
```

Switch2

```
Sw2(config)#router ospf
Sw2(config-ospf-1)#router-id 2.2.2.2
Sw2(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
Sw2(config-ospf-1)#network 11.0.0.0 255.255.255.0 area 0
Sw2(config-ospf-1)#network 12.0.0.0 255.255.255.0 area 0
Sw2(config-ospf-1)#exit
```

Switch3

```
Sw3(config)#router ospf
Sw3(config-ospf-1)#router-id 3.3.3.3
Sw3(config-ospf-1)#network 3.3.3.3 255.255.255.255 area 0
Sw3(config-ospf-1)#network 12.0.0.0 255.255.255.0 area 0
Sw3(config-ospf-1)#exit
```

step 5 Configure BGP&Vxlan

Switch1

```
Sw1(config)#bridge-domain 10
Sw1(config-bridge-domain-10)# vxlan vni 10
Sw1(config-bridge-domain-10)#evpn
Sw1(config-bridge-domain-10)#evpn route-distinguisher 10:1
Sw1(config-bridge-domain-10)# evpn vpn-target 10:1 import-extcommunity
Sw1(config-bridge-domain-10)#evpn vpn-target 10:1 export-extcommunity

Sw1(config)#int 10g 1/0/34.10
Sw1(config)#encapsulation dot1q 10
Sw1(config)#bridge-domain bind 10

Sw1(config-bridge-domain-10)#router bgp 1
Sw1(config-bgp)#router-id 1.1.1.1
Sw1(config-bgp)#neighbor 2.2.2.2 remote-as 1
Sw1(config-bgp)#neighbor 2.2.2.2 update-source 1.1.1.1
Sw1(config-bgp)#ipv4-family unicast
Sw1(config-bgp-af-ipv4)#neighbor 2.2.2.2 enable
Sw1(config-bgp-af-ipv4)#evpn-family
Sw1(config-bgp-af-evpn)#neighbor 2.2.2.2 enable
Sw1(config-bgp-af-evpn)#end
```

Switch2

```
Sw2(config)#bridge-domain 10
Sw2(config-bridge-domain-10)# vxlan vni 10
Sw2(config-bridge-domain-10)#evpn
Sw2(config-bridge-domain-10)#evpn route-distinguisher 10:1
Sw2(config-bridge-domain-10)# evpn vpn-target 10:1 import-extcommunity
Sw2(config-bridge-domain-10)#evpn vpn-target 10:1 export-extcommunity
Sw2(config-bridge-domain-10)#exit

Sw2(config)#bridge-domain 20
Sw2(config-bridge-domain-20)# vxlan vni 20
Sw2(config-bridge-domain-20)#evpn
Sw2(config-bridge-domain-20)#evpn route-distinguisher 20:1
Sw2(config-bridge-domain-20)# evpn vpn-target 20:1 import-extcommunity
Sw2(config-bridge-domain-20)#evpn vpn-target 20:1 export-extcommunity
```

```
Sw2(config-bridge-domain-20)#exit

Sw2(config)#router bgp 1
Sw2(config-bgp)#router-id 2.2.2.2
Sw2(config-bgp)#neighbor 1.1.1.1 remote-as 1
Sw2(config-bgp)#neighbor 1.1.1.1 update-source 2.2.2.2
Sw2(config-bgp)#neighbor 3.3.3.3 remote-as 1
Sw2(config-bgp)#neighbor 3.3.3.3 update-source 2.2.2.2
Sw2(config-bgp)#ipv4-family unicast
Sw2(config-bgp-af-ipv4)#neighbor 1.1.1.1 enable
Sw2(config-bgp-af-ipv4)#neighbor 3.3.3.3 enable
Sw2(config-bgp-af-ipv4)# evpn-family
Sw2(config-bgp-af-evpn)#neighbor 2.2.2.2 enable
Sw2(config-bgp-af-evpn)#end
```

Switch3

```
Sw3(config)#bridge-domain 20
Sw3(config-bridge-domain-20)# vxlan vni 20
Sw3(config-bridge-domain-20)#evpn
Sw3(config-bridge-domain-20)#evpn route-distinguisher 20:1
Sw3(config-bridge-domain-20)# evpn vpn-target 20:1 import-extcommunity
Sw3(config-bridge-domain-20)#evpn vpn-target 20:1 export-extcommunity
Sw3(config-bridge-domain-20)#exit

Sw3(config)#int 10g 1/0/58.20
Sw3(config)#encapsulation dot1q 20
Sw3(config)#bridge-domain bind 20

Sw3(config)#router bgp 1
Sw3(config-bgp)# router-id 3.3.3.3
Sw3(config-bgp)#neighbor 2.2.2.2 remote-as 1
Sw3(config-bgp)#neighbor 2.2.2.2 update-source 3.3.3.3
Sw3(config-bgp)#ipv4-family unicast
Sw3(config-bgp-af-ipv4)#neighbor 2.2.2.2 enable
Sw3(config-bgp-af-ipv4)#evpn-family
Sw3(config-bgp-af-evpn)#neighbor 2.2.2.2 enable
Sw2(config-bgp-af-evpn)#end
```

step 6 Create a VXLAN tunnel on switch1,switch2 and switch3

Switch1

```
Sw1#configure
Sw1(config)#interface nve 1
Sw1(config-nve-1)#tunnel source 1.1.1.1
Sw1(config-nve-1)#vni 10 replication-protocol bgp
```

Switch2

```
Sw2#configure
Sw2(config)#interface nve 1
Sw2(config-nve-1)#tunnel source 2.2.2.2
Sw2(config-nve-1)#vni 10 replication-protocol bgp
Sw2(config-nve-1)#vni 20 replication-protocol bgp
```

Switch3

```
Sw3#configure
Sw3(config)#interface nve 1
Sw3(config-nve-1)#tunnel source 3.3.3.3
Sw3(config-nve-1)#vni 20 replication-protocol bgp
```

step 7 Confiugre BDIF on switch2

Switch2

```
Sw2(config)#int bridge-domain 10
Sw2(config-bridge-domain10)#ip address 192.168.10.254/24

Sw2(config)#int bridge-domain 20
Sw2(config-bridge-domain20)#ip address 192.168.20.254/24
```

12.2.3 Distributed VXLAN Gateway Configuration in BGP EVPN mode

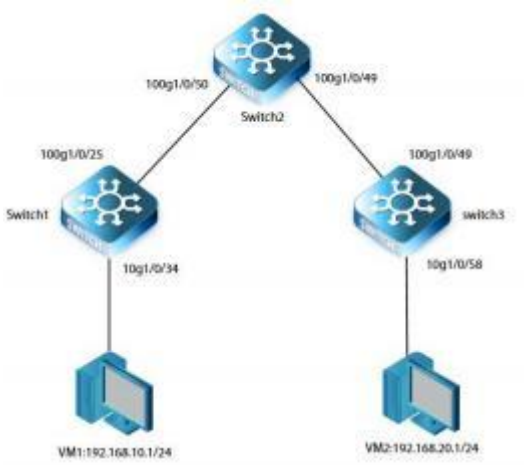


Figure 12-3 Distributed VXLAN Gateway in BGP EVPN mode

The following configurations are same on Switch1 ,Switch2 and Switch3：

step 1 Enter the configure mode

```
switch#configure
```

step 2 Create vlans

Switch1

```
Sw1(config)#vlan 10,11
Sw1(config)#
```

Switch2

```
Sw2(config)#vlan 11,12
Sw2(config)#
```

Switch3

```
Sw3(config)#vlan 12,20
Sw3(config)#
```

step 3 Enter the interfaceconfigure mode and configure interface properties

Switch1

```
Sw1(config)#int vlan 11
Sw1(config-vlanif-11)#ip address 11.0.0.1/24

Sw1(config-vlanif-11)#int 100g 1/0/25
Sw1(config-100g 1/0/25)#port hybrid vlan 11 tagged
Sw1(config-100g 1/0/25)#exit

Sw1(config)#int loopback 1
Sw1(config)#ip address 1.1.1.1/32
```

Switch2

```
Sw2(config)#int vlan 11
Sw2(config-vlanif-11)#ip address 11.0.0.2/24

Sw2(config-vlanif-11)#int 100g 1/0/50
Sw2(config-100g 1/0/50)#port hybrid vlan 11 tagged
Sw2(config-100g 1/0/50)#exit

Sw2(config)#int vlan 12
Sw2(config-vlanif-12)#ip address 12.0.0.2/24

Sw2(config-vlanif-12)#int 100g 1/0/49
Sw2(config-100g 1/0/49)#port hybrid vlan 12 tagged

Sw2(config-100g 1/0/49)#int loopback 1
Sw2(config-100g 1/0/49)#ip address 2.2.2.2/32
```

Switch3

```
Sw3(config)#int vlan 12
Sw3(config-vlanif-12)#ip address 12.0.0.1/24

Sw3(config-vlanif-12)#int 100g 1/0/49
```

```
Sw3(config-100g 1/0/49)#port hybrid vlan 12 tagged

Sw3(config-100g 1/0/49)#int loopback 1
Sw3(config-100g 1/0/49)#ip address 3.3.3.3/32
```

step 4 Configure switch1,switch2 and switch3 communicate at underlay through ospf

Switch1

```
Sw1(config)#router ospf
Sw1(config-ospf-1)#router-id 1.1.1.1
Sw1(config-ospf-1)#network 1.1.1.1 255.255.255.255 area 0
Sw1(config-ospf-1)#network 11.0.0.0 255.255.255.0 area 0
Sw1(config-ospf-1)#exit
```

Switch2

```
Sw2(config)#router ospf
Sw2(config-ospf-1)#router-id 2.2.2.2
Sw2(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
Sw2(config-ospf-1)#network 11.0.0.0 255.255.255.0 area 0
Sw2(config-ospf-1)#network 12.0.0.0 255.255.255.0 area 0
Sw2(config-ospf-1)#exit
```

Switch3

```
Sw3(config)#router ospf
Sw3(config-ospf-1)#router-id 3.3.3.3
Sw3(config-ospf-1)#network 3.3.3.3 255.255.255.255 area 0
Sw3(config-ospf-1)#network 12.0.0.0 255.255.255.0 area 0
Sw3(config-ospf-1)#exit
```

step 5 Configure BGP&Vxlan

Switch1

Configure BD and a service access point

```
Sw1(config)#bridge-domain 10
Sw1(config-bridge-domain-10)# vxlan vni 10
Sw1(config-bridge-domain-10)#evpn
Sw1(config-bridge-domain-10)#evpn route-distinguisher 10:1
Sw1(config-bridge-domain-10)# evpn vpn-target 10:1 import-extcommunity
Sw1(config-bridge-domain-10)#evpn vpn-target 10:1 export-extcommunity

Sw1(config)#int 10g 1/0/34.10
Sw1(config)#encapsulation dot1q 10
Sw1(config)#bridge-domain bind 10
```

Configure L3VPN

```
Sw1(config)#ip vpn-instance vpn1
Sw1(config-vpn-instance-1)#vxlan vni 500
Sw1(config-vpn-instance-1)#ipv4-family route-distinguisher 500:1
Sw1(config-vpn-instance-1)#vpn-target 500:1 import-extcommunity
Sw1(config-vpn-instance-1)#vpn-target 500:1 export-extcommunity
Sw1(config-vpn-instance-1)#exit
```

Configure BGP

```
Sw1(config)#router bgp 1
Sw1(config-bgp)#router-id 1.1.1.1
Sw1(config-bgp)#neighbor 3.3.3.3 remote-as 1
Sw1(config-bgp)#neighbor 3.3.3.3 update-source 1.1.1.1
Sw1(config-bgp-af-ipv4)#ipv4-family unicast
Sw1(config-bgp-af-ipv4)#neighbor 3.3.3.3 enable
Sw1(config-bgp-af-ipv4)#evpn-family
Sw1(config-bgp-af-evpn)#neighbor 3.3.3.3 enable
Sw1(config-bgp-af-evpn)#ipv4-family vpn-instance vpn1
Sw1(config-bgp-af-ipv4-1)#advertise l2vpn evpn
Sw1(config-bgp-af-ipv4-1)#redistribute connected
Sw1(config-bgp-af-ipv4-1)#end
```

Switch3

Configure BD and a service access point

```
Sw3(config)#bridge-domain 20
Sw3(config-bridge-domain-20)#vxlan vni 20
Sw3(config-bridge-domain-20)#evpn
Sw3(config-bridge-domain-20)#evpn route-distinguisher 20:1
Sw3(config-bridge-domain-20)#evpn vpn-target 20:1 import-extcommunity
Sw3(config-bridge-domain-20)#evpn vpn-target 20:1 export-extcommunity

Sw3(config)#int 10g 1/0/58.20
Sw3(config)#encapsulation dot1q 20
Sw3(config)#bridge-domain bind 20
```

Configure L3VPN

```
Sw3(config)#ip vpn-instance vpn1
Sw3(config-vpn-instance-1)#vxlan vni 500
Sw3(config-vpn-instance-1)#ipv4-family route-distinguisher 500:1
Sw3(config-vpn-instance-1)#vpn-target 500:1 import-extcommunity
Sw3(config-vpn-instance-1)#vpn-target 500:1 export-extcommunity
Sw3(config-vpn-instance-1)#exit
```

Configure BGP

```
Sw3(config)#router bgp 1
Sw3(config-bgp)#router-id 1.1.1.1
Sw3(config-bgp)#neighbor 3.3.3.3 remote-as 1
Sw3(config-bgp)#neighbor 3.3.3.3 update-source 1.1.1.1
```

```
Sw3(config-bgp-af-ipv4)#ipv4-family unicast
Sw3(config-bgp-af-ipv4)#neighbor 3.3.3.3 enable
Sw3(config-bgp-af-ipv4)#evpn-family
Sw3(config-bgp-af-evpn)#neighbor 3.3.3.3 enable
Sw3(config-bgp-af-evpn)#ipv4-family vpn-instance vpn1
Sw3(config-bgp-af-ipv4-1)#advertise l2vpn evpn
Sw3(config-bgp-af-ipv4-1)#redistribute connected
Sw3(config-bgp-af-ipv4-1)#end
```

step 6 Create a VXLAN tunnel on switch1 and switch3

Switch1

```
Sw1(config)#interface nve 1
Sw1(config)#tunnel source 1.1.1.1
Sw1(config)#vni 10 replication-protocol bgp
```

Switch3

```
Sw3(config)#interface nve 1
Sw3(config)#tunnel source 3.3.3.3
Sw3(config)#vni 20 replication-protocol bgp
```

step 7 Confiugre BDIF on switch2

Switch1

```
Sw1(config)#int bridge-domain 10
Sw1(config-bridge-domain10)#ip binding vpn-instance vpn1
Sw1(config-bridge-domain10)#ip address 192.168.10.254/24
```

Switch3

```
Sw3(config)#int bridge-domain 20
Sw1(config-bridge-domain20)#ip binding vpn-instance vpn1
Sw1(config-bridge-domain20)#ip address 192.168.20.254/24
```

12.3 Application cases

N/A

13 Reliability Configuration Guide

13.1 Configuring G.8032

13.1.1 Overview

Function Introduction

This document describes the configuration of G.8032 Ethernet Ring Protection Switching.

Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. Each ring node is connected to adjacent nodes participating in the same ring, using two independent links. A ring link is bounded by two adjacent nodes and a port for a ring link is called a ring port. The minimum number of nodes on a ring is two.

Two basic problems to be solved in ring protection are

- Prevent a loop ,prevent a broadcast storm
- MAC learning and forwarding mechanisms for data traffic

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked, i.e., not used for traffic. One designated node, the RPL owner, is responsible to block traffic over the RPL. Under a ring failure condition, the RPL owner is responsible to unblock the RPL, allowing the RPL to be used for traffic.

The event of a ring failure results in protection switching of the traffic. The owner is responsible for opening the ring protection link to ensure the network is smooth and the business will not be interrupted.

An APS protocol is used to coordinate the protection actions over the ring.Each node in the loop needs to be configured accordingly.

Principle Description

Reference: ITU-T G.8032/Y.1344 (06/2008)

13.1.2 Configuration

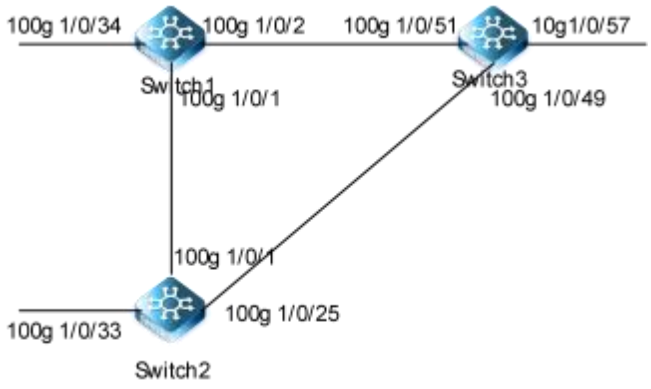


Figure 13-1 G.8032

The following configuration should be operated on all switches if the switch ID is not specified.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Enter the interfaceconfigure mode and create the vlan

```
switch(config)#vlan 100-500
```

step 3 Enter the interface configure mode and set the attributes of the interface

Interface configuration for Switch1:

```
switch1(config)#interface 10gigaethernet 1/0/34
switch1(config-10ge1/0/34)# port link-type trunk
switch1(config-10ge1/0/34)# no port trunk allow-pass vlan 1
switch1(config-10ge1/0/34)# port trunk allow-pass vlan 100-500
switch1(config-10ge1/0/34)#interface 100gigaethernet 1/0/1
switch1(config-100ge1/0/1)# port link-type trunk
switch1(config-100ge1/0/1)# no port trunk allow-pass vlan 1
switch1(config-100ge1/0/1)# port trunk allow-pass vlan 100-500
switch1(config-100ge1/0/1)#interface 100gigaethernet 1/0/2
switch1(config-100ge1/0/2)# port link-type trunk
switch1(config-100ge1/0/2)# no port trunk allow-pass vlan 1
switch1(config-100ge1/0/2)# port trunk allow-pass vlan 100-500
```

Interface configuration for Switch2:

```
switch2(config)#interface 10gigaethernet 1/0/33
switch2(config-10ge1/0/33)# port link-type trunk
switch2(config-10ge1/0/33)# no port trunk allow-pass vlan 1
switch2(config-10ge1/0/33)# port trunk allow-pass vlan 100-500
switch2(config-10ge1/0/33)#interface 100gigaethernet 1/0/25
switch2(config-100ge1/0/25)# port link-type trunk
switch2(config-100ge1/0/25)# no port trunk allow-pass vlan 1
switch2(config-100ge1/0/25)# port trunk allow-pass vlan 100-500
switch2(config-100ge1/0/25)#interface 100gigaethernet 1/0/1
switch2(config-100ge1/0/1)# port link-type trunk
switch2(config-100ge1/0/1)# no port trunk allow-pass vlan 1
switch2(config-100ge1/0/1)# port trunk allow-pass vlan 100-500
```

Interface configuration for Switch3:

```
switch3(config)#interface 10gigaethernet 1/0/57
switch3(config-10ge1/0/57)# port link-type trunk
switch3(config-10ge1/0/57)# no port trunk allow-pass vlan 1
switch3(config-10ge1/0/57)# port trunk allow-pass vlan 100-500
switch3(config-10ge1/0/57)#interface 100gigaethernet 1/0/49
switch3(config-100ge1/0/49)# port link-type trunk
switch3(config-100ge1/0/49)# no port trunk allow-pass vlan 1
```

```
switch3(config-100ge1/0/49)# port trunk allow-pass vlan 100-500
switch3(config-100ge1/0/49)#interface 100gigaethernet 1/0/51
switch3(config-100ge1/0/51)# port link-type trunk
switch3(config-100ge1/0/51)# no port trunk allow-pass vlan 1
switch3(config-100ge1/0/51)# port trunk allow-pass vlan 100-500
```

step 4 Create G.8032 ring node and set the attributes of this node

Note： Each node of the G.8032 major ring has one east-interface and one west interface. These two interfaces have the same role. The east and west interfaces are functionally equivalent.When creating the g. 8032 link point, it is necessary to specify both east-west interfaces;

G.8032 on Switch1

```
Switch1(config)#g8032
Switch1(config-g8032)#show
Switch1(config-g8032)#g8032 instance 1 role rpl-owner-node
Switch1(config-g8032)#g8032 instance 1 rpl port1
Switch1(config-g8032)#g8032 instance 1 channel 100
Switch1(config-g8032)#g8032 instance 1 vlan 101-500
switch(config-g8032)#g8032 instance 1 port1 100g 1/0/1
switch(config-g8032)#g8032 instance 1 port2 100g 1/0/2
```

G.8032 on Switch2

```
switch2(config)#g8032
switch2(config-g8032)# g8032 instance 1 role neighbor
switch2(config-g8032)# g8032 instance 1 rpl port2
switch2(config-g8032)# g8032 instance 1 vlan 101-500
switch2(config-g8032)# g8032 instance 1 channel 100
switch2(config-g8032)#g8032 instance 1 port2 100g 1/0/1
switch2(config-g8032)#g8032 instance 1 port1 100g 1/0/25
```

G.8032 on Switch3

```
switch3(config)#g8032
switch3(config-g8032)#g8032 instance 1 channel 100
switch3(config-g8032)#g8032 instance 1 vlan 101-500
switch3(config-g8032)#g8032 instance 1 port1 100g 1/0/51
switch3(config-g8032)#g8032 instance 1 port2 100g 1/0/49
```

step 5 Exit the configure mode

```
switch(config)# end
```

step 6 Validation

Display the result on Switch1.

```
Switch1(config)#show g8032 instance 1
```

```
g8032 trap:enable
g8032 vs-switch:disable

  Instance:1
        State:Idle
        Mode:revertive
        Role:rpl-owner-node
        Version:v2
        Rpl:port1
        Channel:100
        Mel:0
        VLAN list:101-500
        WTR-timer:5
        Hold-off-timer:0
        Guard-timer:500
        Port1:100ge1/0/1
        Port2:100ge1/0/2
        Virtual Channel:N/A
        Vc-Mel:0
        VC-mep:none
        VC-Hold-off-timer:0
        WTR Remain:0
        Protect Mode:auto
        Protect request port:none
Switch1(config)#
Switch1(config)#show g8032 instance 1 interface
Instance Interface      Role    Type    Operate   Forward     Rx-Count  Tx-Count
1        100ge1/0/1     port1   rpl     working   blocking    61992     688
1        100ge1/0/2     port2   normal  working   forwarding  1094      31531
Switch1(config)#
```

Display the result on Switch2.

```
Switch2(config)#show g8032 instance 1
g8032 trap:enable
g8032 vs-switch:disable

  Instance:1
        State:Idle
        Mode:revertive
        Role:neighbor
        Version:v2
        Rpl:port2
        Channel:100
        Mel:0
        VLAN list:101-500
        WTR-timer:5
        Hold-off-timer:0
```

```
        Guard-timer:500
        Port1:100ge1/0/25
        Port2:100ge1/0/1
        Virtual Channel:N/A
        Vc-Mel:0
        VC-mep:none
        VC-Hold-off-timer:0
        WTR Remain:0
        Protect Mode:auto
        Protect request port:none
Switch2(config)#
Switch2(config)#show g8032 instance 1    interface
Instance Interface          Role      Type      Operate     Forward       Rx-Count   Tx-Count
1            100ge1/0/1         port2     rpl       working     blocking      190          68
1            100ge1/0/25        port1     normal    working     forwarding    190          157
Switch2(config)#
```

Display the result on Switch3.

```
Switch3(config)#show g8032 instance 1
g8032 trap:enable
g8032 vs-switch:disable

  Instance:1
        State:Idle
        Mode:revertive
        Role:none
        Version:v2
        Rpl:none
        Channel:100
        Mel:0
        VLAN list:101-500
        WTR-timer:5
        Hold-off-timer:0
        Guard-timer:500
        Port1:100ge1/0/51
        Port2:100ge1/0/49
        Virtual Channel:N/A
        Vc-Mel:0
        VC-mep:none
        VC-Hold-off-timer:0
        WTR Remain:0
        Protect Mode:auto
        Protect request port:none
Switch3(config)#
Switch3(config)#show g8032 instance 1 interface
Instance Interface          Role      Type      Operate     Forward       Rx-Count   Tx-Count
1            100ge1/0/49        port2     normal    working     forwarding    1336         31535
```

```
1          100ge1/0/51      port1    normal  working   forwarding  63068     677
Switch3(config)#
```

13.1.3 Application cases

N/A

13.2 Configuring UDLD

13.2.1 Overview

Function Introduction

UDLD (Unidirectional Link Detection) is a lightweight protocol that can detect and disable one-way links. By using UDLD, you can prevent exceptions that can arise when a protocol such as a spanning tree is used for a one-way link.

Principle Description

N/A

13.2.2 Configuration

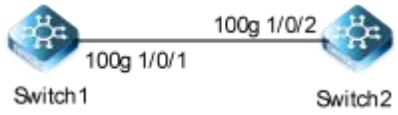


Figure 13-2 UDLD

The following configurations are same on Switch1 and Switch2.

step 1 Enter the configure mode

```
Switch# configure
```

step 2 Enter the interface configure mode and enable udld

```
switch(config)# interface 10g 1/0/1
switch(config-10ge1/0/1)#udld enable
```

step 3 Enable udld globally

```
switch(config)#udld work-mode normal
```

step 4 Set the message interval (optional)

If the message is not specified, use the default value: 7 seconds.

```
switch(config)#udld advertise-interval 10
```

step 5 Exit the configure mode

```
Switch(config)# end
```

step 6 Check the configuration

switch1:

```
switch#show udld interface
UDLD interface information:
 Interface : 10gigaethernet 1/0/1
    Udld status : enable
    Udld state : advertise
    Udld peer number : 1
    Udld bidirection number : 1
    Udld bidirection state: bidirectional
   Expiration time : 29

switch(config)#show udld local
 UDLD local:
    Work mode : normal
    Shutdown when unidirectional : auto
    Advertisement interval : 10(s)
 Device Id : 3638:3231:3546
    Device name : s2
    Trap status : disable
    Error-down recover : enable
    Error-down recover-time : 45
    Up-delay time : 0
switch (config)#show udld peer
UDLD Peer information:
   Interface : 10gigaethernet 1/0/1
   Mac address: 6821:5fb7:0a10
    Peer State : bidirectional
    Peer Device Id : 3638:3231:3546
    Peer Port Id : 10GigaEthernet1/0/2
    Peer Device Name : Switch
    Peer Message Interval : 7
    Peer Timeout Interval : 5
    Peer Expire Time : 16
```

Switch2：

```
switch(config)#show udld interface
UDLD interface information:
 Interface : 10gigaethernet 1/0/2
    Udld status : enable
    Udld state : advertise
```

```
    Udld peer number : 1
    Udld bidirection number : 1
    Udld bidirection state: bidirectional
Switch(config)#show udld local
 UDLD local:
    Work mode : normal
    Shutdown when unidirectional : auto
    Advertisement interval : 7(s)
 Device Id : 3638:3231:3546
    Device name : Switch
    Trap status : disable
    Error-down recover : enable
    Error-down recover-time : 45
    Up-delay time : 0
Switch(config)#show udld peer
UDLD Peer information:
  Interface : 10gigaethernet 1/0/2
  Mac address: 6821:5fb7:5d10
    Peer State : bidirectional
    Peer Device Id : 3638:3231:3546
    Peer Port Id :10GigaEthernet1/0/1
    Peer Device Name : s2
    Peer Message Interval : 10
    Peer Timeout Interval : 5
    Peer Expire Time : 13
```

13.2.3 Application cases

N/A

13.3 Configuring FLink

13.3.1 Overview

Function Introduction

The Flexible-Link is a simple but practical technology of fast link protection. It is a solution specific to dual uplink networking to fulfill redundancy and fast migration of active and standby links.

Every Flexible-Link group is included a pair of a layer 2 interfaces where one interface is configured to act as a standby to the other. The feature provides an alternative solution to the STP. Users can disable STP and still retain basic link redundancy. The feature also support load-balancing so than both interfaces simultaneously forward the traffic.

Principle Description

N/A

13.3.2 Configuration

Single type Configuration

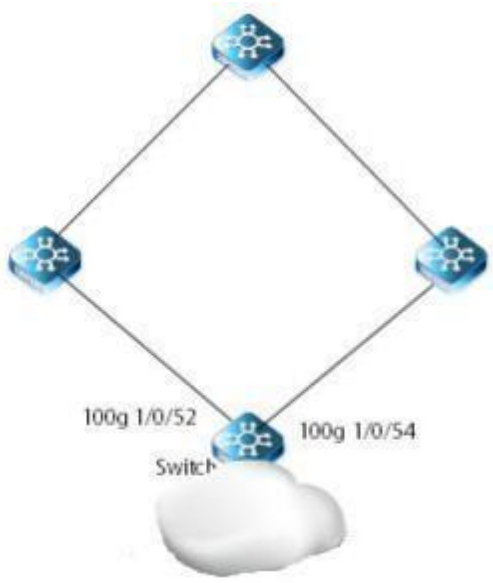


Figure 13-3 Flexible-Link single type

The figure above is a typical Flexible-Link single type topo. The Switch is configured with a FLINK group.

The following example shows the configuration of dual uplink protection for FLink links, with a protected vlan of 1000,100g1/0/52 directly connected to the primary link and 100g1/0/54 directly connected to the standby link.

To configure smart-link group, some configurations should be configured before it.

- VLANs should be configured.
- Spanning-tree should be disabled in the interface.

The following configuration should be operated on all switches if the switch ID is not specified.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create a vlan

```
switch(config)# vlan 1000
switch(vlan-1000)# exit
```

step 3 Configure related interfaces to allow the vlan to pass through

```
switch(config)#int 100g 1/0/54
switch(config-100ge1/0/54)#port hybrid vlan 1000 tagged
```

```
switch(config-100ge1/0/54)#int 100g 1/0/52
switch(config-100ge1/0/52)#port hybrid vlan 1000 tagged
switch(config-100ge1/0/52)#quit
```

step 4 Create a RLINK group and specify the master and slave interfaces

```
switch(config)#flink group 1
switch(config-flink1)#protect-vlan 1000
switch(config-flink1)#add interface 100g 1/0/54 role master
switch(config-flink1)#add interface 100g 1/0/52 role slave
switch(config-flink1)#quit
```

step 5 Exit the configuration mode

```
switch(config)# end
```

step 6 Verify the configuration

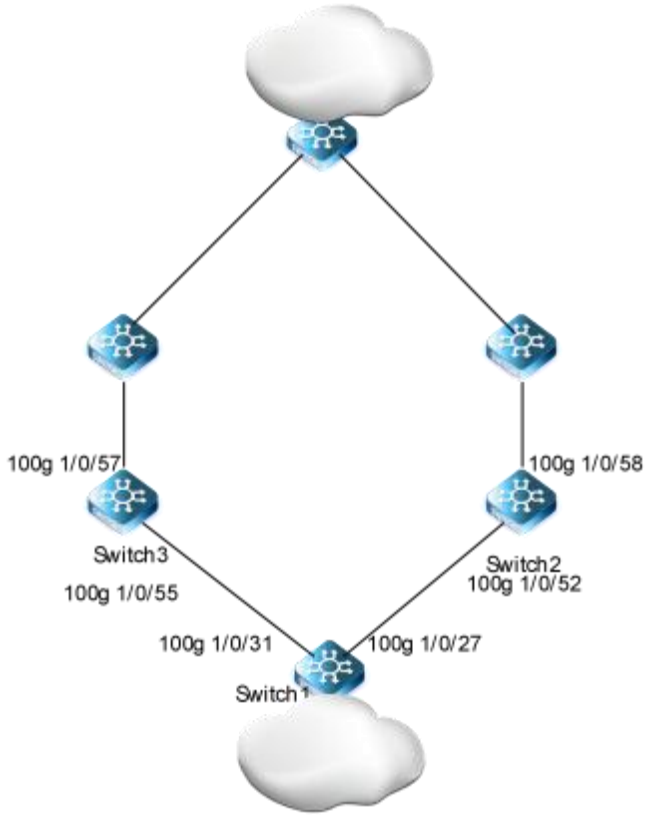
```
switch(config)#show flink config
Version:FLINK_VB3.00.02.00
!
flink group 1
 protect-vlan 1000
 reverse enable
 reverse time 0
 snmp-trap enable

 interface 100ge1/0/52
 join flink group 1 role slave

 interface 100ge1/0/54
 join flink group 1 role master.
switch(config)#show flink group
  <cr>
  <1-8>  flink group number
switch2(config)#show flink group 1
flink group 1 information:
  Group status          : active
  Group type            : single
  Group vlanlist        : 1000
  Reverse               : disable
  Reverse time          : 0s
  Snmp trap             : disable

  Member                Role    State     Status    Linkstate
  100ge1/0/52           slave   forward   active    up/up
  100ge1/0/54           master  block     active    up/up
```

Double type Configuration



Ffigure 13-4 Flexible-Link double type

The figure above is a typical Flexible-Link double type topo. The switch2 and switch3 are configured with FLINK groups.

The following example shows the configuration of FLink double uplink protection with a protected VLAN of 1000, a health VLAN of 1001, a primary link on Switch3, and a standby link on Switch2.

To configure flink, some configurations should be configured before it.

- VLANs should be configured.
- Spanning-tree should be disabled in the interface.

The following configuration should be operated on all switches if the switch ID is not specified.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create vlans and configure related interfaces to allow the vlan to pass through

```
switch1(config)# vlan 1000-1001
switch1(config)# interface 100gigaethernet 1/0/31
switch1(config-100ge1/0/31)#port hybrid vlan 1000,1001 tagged
switch1(config-100ge1/0/31)#interface 100gigaethernet 1/0/27
```

```
switch1(config-100ge1/0/27)#port hybrid vlan 1000,1001 tagged
```

Switch2 Confgurations

```
switch2(config)# vlan 1000-1001
switch2(config-100ge1/0/55)#po hybrid vlan 1000,1001 tagged
switch2(config-100ge1/0/55)#interface 10g 1/0/57
switch2(config-10ge1/0/57)#port hybrid vlan 1000 tagged
switch2(config-10ge1/0/57)#quit
```

Switch3 Configurations

```
switch3(config)#vlan 1000-1001
switch2(config-100ge1/0/52)#po hybrid vlan 1000,1001 tagged
switch2(config-100ge1/0/52)#interface 10g 1/0/58
switch2(config-10ge1/0/58)#port hybrid vlan 1000 tagged
switch2(config-10ge1/0/58)#quit
```

step 3 Create RLINK groups and specify the master and sender interfaces on switch3,specify the slave and sender interfaces on switch2

Switch2 Confgurations

```
switch2(config)#flink group 1
switch2(config-flink1)#type double
switch2(config-flink1)#protect-vlan 1000
switch2(config-flink1)#add int 10g 1/0/57 role slave
switch2(config-flink1)#add interface 100g 1/0/55 role sender
```

Switch3 Configurations

```
switch3(config)#flink group 1
switch3(config-flink1)#type double
switch3(config-flink1)#protect-vlan 1000
switch3(config-flink1)#add interface 100g 1/0/55 role sender
switch3(config-flink1)#add interface 10g 1/0/57 role master
```

step 4 Exit the configuration mode

```
switch(config)# end
```

step 5 Verify the configurations

Verify the configurations on switch2

```
 switch2(config)#show flink config
Version:FLINK_VB3.00.02.00
!
flink group 1
 type double
```

```
 protect-vlan 1000
 reverse enable
 reverse time 0
 snmp-trap enable

 interface 100ge1/0/52
join flink group 1 role sender

 interface 10ge1/0/58
join flink group 1 role slave



switch2(config)#show flink group 1
flink group 1 information:
  Group status              : active
  Group type                : double
  Group vlanlist            : 1000
  Reverse                   : disable
  Reverse time              : 0s
  Snmp trap                 : disable
  Receive timeout           : 15multiple
  Send interval             : 1000ms
  Peer exist                : exist
  Peer mac                  : 68:21:5f:ffffffdb:fffffffc:00
  Peer role                 : master
  Peer state                : forward
  PeerReverse               : disable
  Peer send interval        : 1000
  Peer linkstate            : up

  Member                 Role     State      Sendvlan  Status     Linkstate
  100ge1/0/52            sender   forward    0         active     up/up
  10ge1/0/58             slave    block      0         active     up/up
```

Verify the configurations on switch3

```
switch3(config)#show flink config
Version:FLINK_VB3.00.02.00
!
flink group 1
 type double
 protect-vlan 1000
 reverse enable
 reverse time 0
 snmp-trap enable

 interface 100ge1/0/55
join flink group 1 role sender
```

```
 interface 10ge1/0/57
join flink group 1 role master

switch3(config)#show flink group
flink group 1 information:
  Group status              : active
  Group type                : double
  Group vlanlist            : 1000
  Reverse                   : disable
  Reverse time              : 0s
  Snmp trap                 : disable
  Receive timeout           : 15multiple
  Send interval             : 1000ms
  Peer exist                : exist
  Peer mac                  : 68:21:5f:ffffffb7:5b:10
  Peer role                 : slave
  Peer state                : block
  PeerReverse               : disable
  Peer send interval        : 1000
  Peer linkstate            : up

  Member                    Role    State     Sendvlan  Status    Linkstate
  100ge1/0/55               sender  forward   0         active    up/up
  10ge1/0/57                master  forward   0         active    up/up
```

13.4 Configuring Monitor Link

13.4.1 Overview

Function Introduction

Monitor Link is a port collaboration function. Monitor Link usually works together with Layer 2 topology protocols. The idea is to monitor the states of uplink ports and adapt the up/down state of downlink ports to the up/down state of uplink ports, triggering link switch over on the downstream switch in time.

Principle Description

N/A

13.4.2 Configuration

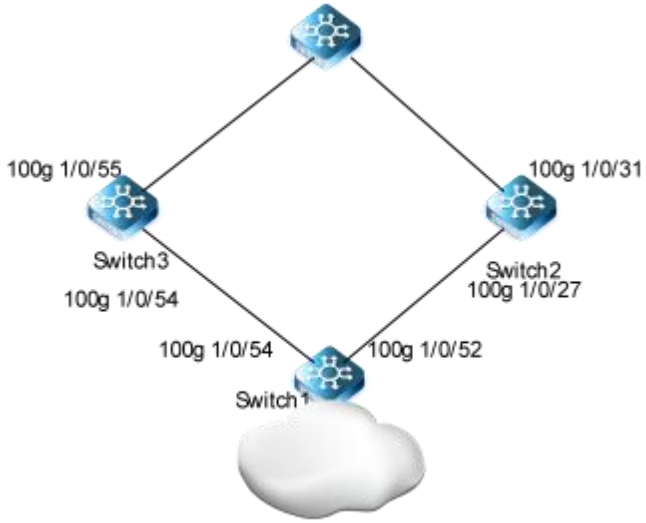


Figure 13-5 monitor link

The figure above is a typical topo for combining Monitor Link and Flexible Link on a network. The switch1 and switch3 are configured with Mlink groups.

To configure flink, some configurations should be configured before it.

- Spanning-tree should be disabled in the interface.

The following configuration should be operated on all switches if the switch ID is not specified.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create a MLINK group and configurate uplink and downlink interfaces

```
switch3(config)#mlink group 1
switch3(config-mlink1)#add interface 100g 1/0/54 role downlink
switch3(config-mlink1)#add interface 100g 1/0/55 role uplink
switch3(config-mlink1)#quit
```

step 3 Exit the configuration mode

```
switch(config)# end
```

step 4 Verify the configurations

```
switch3(config)#show mlink config
Version:MLINK_VB3.00.01.00
!
mlink group 1
```

```
!
interface 100gigaethernet 1/0/54
 join mlink group 1 role downlink
!
interface 100gigaethernet 1/0/55
 join mlink group 1 role uplink

switch3(config)#show mlink group 1
Mlink group 1 information:
  Group status: active
  Snmp trap : disable
  Uplink-select : first-up
  Hold off time : 3
  Member              Role          State      Status     Linkstate
  100ge1/0/54         DOWNLINK      FORWARD    ACTIVE     up/up
  100ge1/0/55         UPLINK        FORWARD    ACTIVE     up/up
```

13.4.3 Application cases

N/A

13.5 Configuring VRRP

13.5.1 Overview

Function Introduction

This chapter provides an overview of Virtual Router Redundancy Protocol (VRRP) and its implementation. VRRP eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. One of the major advantages of VRRP is that it makes default path available without requiring configuration of dynamic routing on every end-host.

Note： MD5 authentication is not yet supported for VRRP.

Principle Description

The VRRP module is based on: RFC 3768 (VRRP): Knight, S., et.al "Virtual Router Redundancy Protocol (VRRP)"

Terminology

Backup Router： VRRP router that back up an IP address. It assumes forwarding responsibility for the virtual IP address if the Master fails.

IP Address Owner： The VRRP Router that has the virtual router's IP address (es) as real interface address (es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, etc.

Master Router： The VRRP router that owns the IP address (i.e., is being backed up), and which is the default router for forwarding for that IP address.

Virtual IP： The IP address back up by a VRRP session.

Virtual Router： A router managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP addresses across a common LAN. A VRRP Router might backup one or more virtual routers.

VRRP Router： A router runs the Virtual Router Redundancy Protocol. It might participate in one or more virtual routers.

VRID: Virtual router ID.

Virtual MAC address: MAC address that is generated by the virtual router based on the VRID. The virtual router sends ARP Reply packets carrying the virtual MAC address but not the interface MAC address.

Typically, terminal hosts are connected to the enterprise network through a single router (first hop router) that is in the same Local Area Network (LAN) segment. The most popular method of configuration for the end hosts is to statically configure this router as their default gateway. This minimizes configuration and processing overhead. The main problem with this configuration method is that it produces a single point of failure if this first hop router fails.

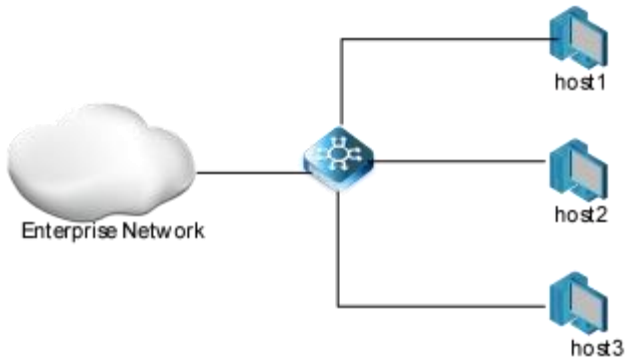


Figure 13-6 Without VRRP

The Virtual Router Redundancy Protocol attempts to solve this problem by introducing the concept of a virtual router, composed of two or more VRRP routers on the same subnet. The concept of a virtual IP address is also introduced, which is the address that end hosts configure as their default gateway. Only one router (called the master) forward packets on the behalf of this IP address. In the event that the Master router fails, one of the other routers (Backup) assumes forwarding responsibility for it.

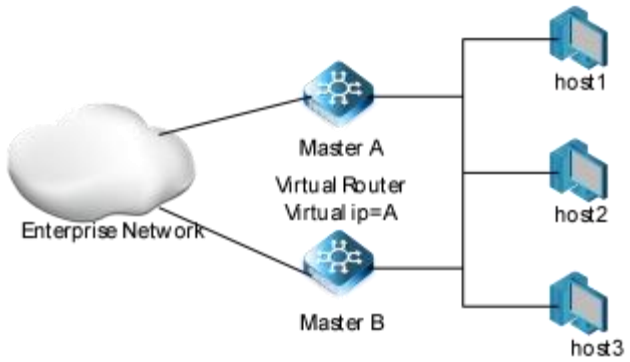


Figure 13-7 With VRRP

At first glance, the configuration outlined in might not seem very useful, as it doubles the cost and leaves one router idle at all times. This, however, can be avoided by creating two virtual routers and splitting the traffic between them.

13.5.2 Configuration

Configuring VRRP (One Virtual Router)

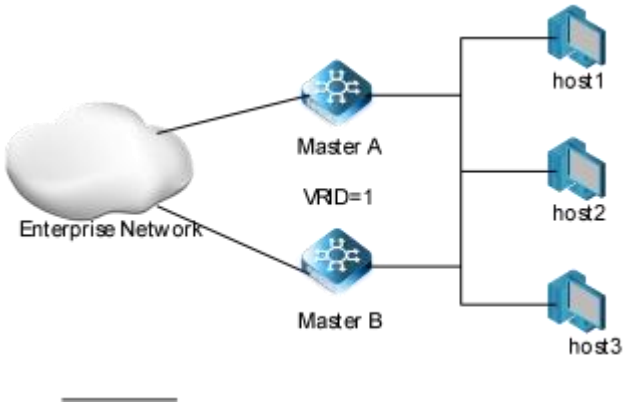


Figure 13-8 VRRP with one virtual router

The primary and backup mode means that the service is only undertaken by the Master router.When the Master router fails, a replacement will be selected from the other Backup routers.The primary and backup mode requires only one backup group, in which different routers have different priorities, and the router with the highest priority will become the Master router.

In this configuration the end-hosts install a default route to the IP address of virtual router 1(VRID = 1) and both routers R1 and R2 run VRRP. R1 is configured to be the Master for virtual router 1 (VRID = 1) and R2 as a Backup for virtual router 1. If R1 fails, R2 will take over virtual router 1 and its IP addresses, and provide uninterrupted service for the hosts. Configuring only one virtual router, doubles the cost and leaves R2 idle at all times.

The following configuration should be operated on all devices if the device ID is not specified.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Create a vlan and configure releated interfaces to allow the vlan to pass through. Assign an IP address to each interfaces

Configure the interface of the Master 1

```
switch1(config)#vlan 1000
switch1(vlan-1000)#int 100g 1/0/31
switch1(config-100ge1/0/31)#port hybrid vlan 1000 tagged
switch1(config-100ge1/0/31)#int vlan 1000
switch1(config-vlanif-1000)#ip add 100.1.1.1/24
switch1(config-vlanif-1000)#quit
```

Configure the interfaces of the Backup 2

```
switch2(config)#vlan 1000
switch2(vlan-1000)#int 100g 1/0/52
switch2(config-100ge1/0/52)#port hybrid vlan 1000 tagged
switch2(config-100ge1/0/52)#int vlan 1000
```

```
switch2config-vlanif-1000)#ip add 100.1.1.2/24
switch2(config-vlanif-1000)#quit
```

step 3 Create a vrrp instance

```
switch(config-vlanif-1000)#ip vrrp 1
switch(config-vlanif-1000)#ip vrrp 1 associate-address 100.1.1.100
```

step 4 Setting the priority in a vrrp instance(optional)

Setting the Device Master1 (switch1)priority as 200 in vrrp 1

```
switch(config-vlanif-1000)#ip vrrp 1 priority 200
```

step 5 Exit the configuration mode

```
switch(config)# end
```

step 6 Verify the configurations

```
switch1(config)#show ip vrrp
  Interface          VRID Role    Version VR-State Pri IP-Count State      Auth-Mode  Auth-Key
  vlan1000           1    normal  2       Master   200 1        Active     none       N/A
```

13.5.3 Application cases

N/A

13.6 Configuring IP BFD

13.6.1 Overview

Function Introduction

An increasingly important feature of networking equipment is the rapid detection of communication failures between adjacent systems, in order to more quickly establish alternative paths. Detection can come fairly quickly in certain circumstances when data link hardware comes into play (such as Synchronous Optical Network (SONET) alarms). However, there are media that do not provide this kind of signaling (such as Ethernet), and some media may not detect certain kinds of failures in the path, for example, failing interfaces or forwarding engine components.

Networks use relatively slow "Hello" mechanisms, usually in routing protocols, to detect failures when there is no hardware signaling to help out. The time to detect failures (“Detection Times”) available in the existing protocols is no better than a second, which is far too long for some applications and represents a great deal of lost data at gigabit rates. Furthermore, routing protocol Hellos are of no help when those routing protocols are not in use, and the semantics of detection are subtly different -- they detect a failure in the path between the two routing protocol engines.

The goal of Bidirectional Forwarding Detection (BFD) is to provide low-overhead, short-duration detection of failures in the path between adjacent forwarding engines, including the interfaces, data link(s), and, to the extent possible, the forwarding engines themselves.

An additional goal is to provide a single mechanism that can be used for aliveness detection over any media, at any protocol layer, with a wide range of Detection Times and overhead, to avoid a proliferation of different methods.

Note ： If ethernet CFM mep is configured on a physical port and CFM LM is enabled, at the same time, IP BFD is configured on a vlan interface and the former physical port is a member of the vlan, IP BFD can't work normally. If CFM LM is disabled, IP BFD can work normally.

Principle Description

Reference to RFC 5880 Bidirectional Forwarding Detection (BFD)

13.6.2 Configuration

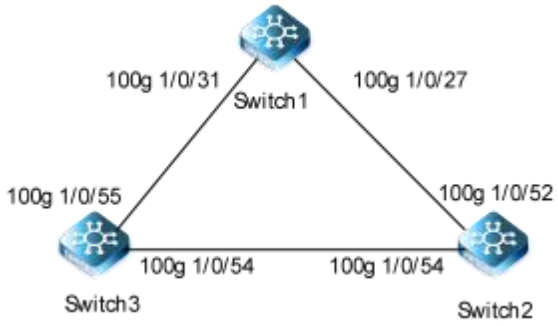


Figure 13-9 BFD single hop

The following configuration should be operated on all switches if the switch ID is not specified.

step 1 Enter the configure mode

```
switch# configure
```

step 2 Configure a static BFD session on Switch1 and Switch2 to monitor the link of the VRRP group.

Interface configuration for Switch1

```
switch1(config)#vlan 1000
switch1(config-100ge1/0/31)#port hybrid vlan 1000 tagged
switch1(config-100ge1/0/31)#no port hybrid vlan 1
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#shutdown
switch1(config-100ge1/0/27)#quit
switch1config)#int vlan 1000
switch1config-vlanif-1000)#ip add 100.1.1.1/24
```

Interface configuration for Switch2

```
switch2(config)#vlan 1000
switch2(config-100ge1/0/54)#port hybrid vlan 1000
tagged switch2(config-100ge1/0/54)#no port hybrid vlan 1
switch2(config-100ge1/0/54)#int 100g 1/0/52
switch2(config-100ge1/0/52)#shutdown
```

```
switch2(config-100ge1/0/52)#quit
switch2(config)#int vlan 1000
switch2(config-vlanif-1000)#ip add 100.1.1.2/24
```

Interface configuration for Switch3

```
switch3(config)#vlan 1000
switch3(vlan-1000)#int 100g 1/0/54
switch3(config-100ge1/0/54)#port hybrid vlan 1000 tagged
switch3(config-100ge1/0/54)#no port hybrid vlan 1
switch3(config-100ge1/0/54)#int 100g 1/0/55
switch3(config-100ge1/0/55)#port hybrid vlan 1000 tagged
switch3(config-100ge1/0/55)#no port hybrid vlan 1
switch3(config-100ge1/0/55)#quit
```

Configurate VRRP groups

```
switch(config-vlanif-1000)#ip vrrp 1
switch(config-vlanif-1000)#ip vrrp 1 associate-address 100.1.1.100
switch1(config-vlanif-1000)#ip vrrp 1 priority 200
```

Configurate a BFD session

```
switch1(config)#bfd start
switch1(config)#bfd track 1 remote-ip 100.1.1.2

switch2(config)#bfd start
switch2(config)#bfd track 1 remote-ip 100.1.1.1
```

Configure association between VRRP and BFD

```
switch2(config-vlanif-1000)# ip vrrp 1 track bfd-session 1 increased 100
```

Verify the configuration

```
switch1(config)#show bfd session
  Interface State Local-Discr Remote-Discr local-addr        remote-addr
  vlan1000   up      1          1          100.1.1.1          100.1.1.2

switch1(config)#show bfd config
Version                       :BFD_VX2.10.00.00
!
bfd start
bfd track 1 remote-ip 100.1.1.2
bfd track 0 min-tx 0 min-rx 0 multiplier 12040167(null)switch1(config)
```

step 3 Configurate BFD for OSPF

Interface configuration for Switch1

```
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#shutdown
```

```
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port hybrid vlan 1000 tagged
switch1(config-100ge1/0/27)#no port hybrid vlan 1
switch1(config-100ge1/0/27)#int vlan 1000
switch1(config-vlanif-1000)#ip add 100.1.1.1/24
```

Interface configuration for Switch2

```
switch2(config)#int 100g 1/0/54
switch2(config-100ge1/0/54)#shutdown
switch2(config-100ge1/0/54)#int 100g 1/0/52
switch2(config-100ge1/0/52)#no port hybrid vlan 1
switch2(config-100ge1/0/52)#port hybrid vlan 1000 tagged
switch2(config-100ge1/0/52)#quit
switch2(config)#int vlan 1000
switch2(config-vlanif-1000)#ip add 100.1.1.2/24
```

Configure the basic OSPF functions

```
switch(config)#router ospf
switch (config-ospf-1)#network 100.1.1.0 255.255.255.0 area 0
```

Configure BFD for OSPF

```
switch(config)#bfd start
switch(config)#int vlan 1000
switch(config-vlanif-1000)#bfd enable
switch(config-vlanif-1000)#ip ospf bfd enable
```

Verify the configuration

```
switch1(config)#show bfd config
Version                          :BFD_VX2.10.00.00
!
bfd start
!
interface vlan 1000
 bfd enable

switch1(config)#show bfd session
  Interface State Local-Discr Remote-Discr local-addr                    remote-addr
  vlan1000   up      1              1              0.0.0.0                      100.1.1.2
```

step 4 Configurate BFD for RIP

Interface configuration for Switch1

```
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#shutdown
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port hybrid vlan 1000 tagged
```

```
switch1(config-100ge1/0/27)#no port hybrid vlan 1
switch1(config-100ge1/0/27)#int vlan 1000
switch1(config-vlanif-1000)#ip add 100.1.1.1/24
```

Interface configuration for Switch2

```
switch2(config)#int 100g 1/0/54
switch2(config-100ge1/0/54)#shutdown
switch2(config-100ge1/0/54)#int 100g 1/0/52
switch2(config-100ge1/0/52)#no port hybrid vlan 1
switch2(config-100ge1/0/52)#port hybrid vlan 1000 tagged
switch2(config-100ge1/0/52)#quit
switch2(config)#int vlan 1000
switch2(config-vlanif-1000)#ip add 100.1.1.2/24
```

Configure the basic RIP functions

```
switch(config)#router rip
switch (config-ospf-1)#network 100.0.0.0
```

Configure BFD for RIP

```
switch(config)#bfd start
switch(config)#int vlan 1000
switch(config-vlanif-1000)#bfd enable
switch(config-vlanif-1000)#ip rip bfd enable
```

Verify the configuration

```
switch1(config-vlanif-1000)#show bfd config
Version                          :BFD_VX2.10.00.00
!
bfd start
!
interface vlan 1000
 bfd enable

switch1(config-vlanif-1000)#show bfd session
  Interface State Local-Discr Remote-Discr local-addr                    remote-addr
  vlan1000   up      1              1              0.0.0.0                 100.1.1.2
```

step 5 Configurate BFD for BGP

Interface configuration for Switch1

```
switch1(config)#int 100g 1/0/31
switch1(config-100ge1/0/31)#shutdown
switch1(config-100ge1/0/31)#int 100g 1/0/27
switch1(config-100ge1/0/27)#port hybrid vlan 1000 tagged
switch1(config-100ge1/0/27)#no port hybrid vlan 1
switch1(config-100ge1/0/27)#int vlan 1000
```

```
switch1(config-vlanif-1000)#ip add 100.1.1.1/24
```

Interface configuration for Switch2

```
switch2(config)#int 100g 1/0/54
switch2(config-100ge1/0/54)#shutdown
switch2(config-100ge1/0/54)#int 100g 1/0/52
switch2(config-100ge1/0/52)#no port hybrid vlan 1
switch2(config-100ge1/0/52)#port hybrid vlan 1000 tagged
switch2(config-100ge1/0/52)#quit
switch2(config)#int vlan 1000
switch2(config-vlanif-1000)#ip add 100.1.1.2/24
```

Configure the basic BGP functions

```
switch1(config)#router bgp 101
switch1(config-bgp)#neighbor 100.1.1.2 remote-as 100

switch2(config)#router bgp 100
switch2(config-bgp)# neighbor 100.1.1.1 remote-as 101
```

Configure BFD for BGP

```
switch1(config)#bfd start
switch1(config)#router bgp
switch1(config-bgp)#neighbor 100.1.1.2 bfd enable

switch2(config)#bfd start
switch2(config)#router bgp
switch2(config-bgp)#neighbor 100.1.1.1 bfd enable
```

Verify the configuration

```
switch1(config-bgp)#show bfd config
Version                          :BFD_VX2.10.00.00
!
bfd start
!
interface vlan 1000
 bfd enable

switch1(config-bgp)#show bfd session
  Interface State Local-Discr Remote-Discr local-addr                                remote-addr

  vlan1000  up      1            1            0.0.0.0                                     100.1.1.2
```

13.6.3 Application cases

N/A

https://www.fs.com