HIRSCHMANN IT

A BELDEN BRAND

User Manual

Configuration

MTS Series Switch

User manual
Release 1.1 04/2020

Technical Support
http://www.belden.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Belden according to the best of the company's knowledge. Belden reserves the right to change the contents of this document without prior notice. Belden can give no guarantee in respect of the correctness or accuracy of the information in this document.

Belden can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.
You can get the latest version of this manual on the Internet at the Hirschmann IT product site (www.belden.com).

Safety agreement

Safety location

By default, device should be placed in certain location that is safe, stable and reliable; all physical operators should be authorized; the operation CLI scripts should be properly kept, updated and reviewed.

Safety channel

Hirschmann IT devices support multiple managing methods, including Telnet, SSH, HTTP, HTTPS and so forth. All un-encrypted management protocols are not recommended. We highly recommend that our user only use SSH and HTTPs as the way to operate the devices, in order to ensure all management traffic is encrypted.

Safety storage

The login credentials, device configuration and status data should be kept in an appropriate place and be updated regularly and this information can only be accessed and managed by authorized people.

Contents

Safety instructions

Warming
UNCONTROLLED MACHINE ACTIONS To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually. Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices. **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

About this Manual

“User manual” contains detailed information about the various functions of operating the device.

Configuration Instruction:

-B -S -E –A Each represents a different version of the software, as follows:

-B: Basic

-S: Standard

-E: Enhanced

-A: Advanced

NOTE: The software performance of 8000 series products is exactly the same as -A products except MPLS QoS.

Maintain

Hirschmann IT has been working to improve and develop software. Check periodically for newer versions of the software to provide you with additional benefits. You can find information and download software from the Hirschmann IT product page on the Internet (www.belden.com).

1 System Operation Basics

1.1 Overview

System operation basics mainly describe the basic knowledge of device operations, including system operation basic functions, device configuration modes, command modes, and command line interface.

1.2 System Operation Basic Functions

Table 1-1 Configuration List of the System Operation Basic Functions

Configuration Task	
Device configuration mode	Device configuration mode
Command operating mode	Command operating mode
Command line interface	Command line interface

1.2.1 Device Configuration Modes *-B -S -E -A*

Users can log in to the device for configuration and management in different modes. (For details of the login modes, refer to the chapter "System login" in the configuration guide.) The device provides four typical configuration modes:

- Logging in to the device locally through the Console port. By default, users can configure the device directly in this mode.
- Logging in to the device by remote dial-up through a Modem. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.
- Logging in to the device remotely through Telnet. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.
- Logging in to the device remotely through SSH. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.

1.2.2 Command Operating Modes *-B -S -E -A*

The device provides a command processing subsystem for management and execution of system commands. The subsystem shell provides the following main functions:

- Registration of system commands
- Editing of system configuration commands by users
- Parsing of the commands that have been inputted by users
- Execution of system commands

If a user configures the device through shell commands, the system provides multiple operating modes for the execution of the commands. Each command mode supports specific configuration commands. In this way, hierarchical protection is provided to the system, protecting the system from unauthorized access.

The shell subsystem provides multiple modes for the operating of configuration commands. These modes have different system prompts, prompting the current system mode of the user. The following lists common configuration modes:

- Common user mode (user EXEC)
- Privileged user mode (privilege EXEC)
- Global configuration mode (global configuration)
- Interface configuration mode (interface configuration)
- File system configuration mode (file system configuration)
- Access list configuration mode (access list configuration)
- Other configuration modes (They will be described in the related sections and chapters.)

The following table shows how to enter the common command modes and switch over between the modes.

Table 1-2 System Modes and Methods of Switching Over Between the Modes

Mode	How to Enter the Mode	System Prompt	How to Exit the Mode	Functions
Common user mode	Log in to the device.	Hostname>	Run the **exit** command to exit the mode.	Changes the terminal settings. Performs basic tests. Display the system information.
Privileged user mode	In common user mode, run the **enable** command.	Hostname#	Run the **disable** or **exit** command to exit to the common user mode.	Configure the operating parameters of the device.

Mode	How to Enter the Mode	System Prompt	How to Exit the Mode	Functions
				Display the operating information of the device.
Global configuration mode	In privileged user mode, run the **configure terminal** command.	Hostname (config)#	Run the **exit** command to exit to the privileged user mode.	Configures the global parameters that are required for the device operation.
Interface configuration mode	In global configuration mode, run the **interface** command (while specifying the corresponding interface or interface group).	Hostname(config-if-xxx[number])# or Hostname(config-if-group[number])#	Run the **exit** command to exit to the global configuration mode. Run the **end** command to exit to the privileged user mode.	In this mode, configures device interfaces, including: Interfaces of different types Interface groups
File system configuration mode	In the privileged user mode, run the **filesystem** command.	Hostname(config-fs)#	Run the **exit** command to exit to the privileged user mode.	Manages the file system of the device.
Access list configuration mode	In global configuration mode, run the **ip access-list standard** or **ip access-list extended** command.	Hostname(config-std-nacl)# Hostname(config-ext-nacl)#	Run the **exit** command to exit to the global configuration mode. Run the **end** command to exit to the privileged user mode.	Configures the Access Control List (ACL). The configuration tasks include: Configuring standard access control lists. Configuring extended access control lists.

NOTE

- Hostname is the system name. In global configuration mode, a user can run the **hostname** command to modify the system name, and the modification takes effect immediately.
- If a user is not in privileged user mode while the user wants to run a privileged mode command, the user can use the **do** command to run the required command without the need to returning back to the privileged mode. (For details, refer to the related sections in "System Operation Basics" of the command manual.) Note that the mode switchover command such as **do configure terminal** is not included.

1.2.3 Command Line Interface *-B -S -E -A*

The command line interface is a man-machine interface that is provided by the shell subsystem to configure and use the device. Through the command line interface, users can input and edit commands to perform the required configuration tasks, and they can also query the system information and learn the system operation status.

The command line interface provides the following functions for the users:

- System help information management
- System command inputting and editing
- History command management
- Terminal display system management

Command Line Online Help

The command line provides the following types of online help:

- Help
- Full help
- Partial help

Through the above types of online help, users can obtain various help information. The following gives some examples.

- To obtain a brief description of the online help system, enter the **help** command in any command mode.

```
Hostname#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help for command are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
And "Edit key" usage is the following:
   CTRL+A -- go to home of current line
   CTRL+E -- go to end of current line
   CTRL+U -- erase all character from home to current cursor
   CTRL+K -- erase all character from current cursor to end
   CTRL+W -- erase a word on the left of current cursor
```

```
  CTRL+R -- erase a word on the right of current cursor
  CTRL+D,DEL -- erase a character on current cursor
  BACKSPACE -- erase a character on the left of current cursor
  CTRL+B,LEFT -- current cursor backward a character
  CTRL+F,RIGHT -- current cursor forward a character
```

- To list all commands and their brief description in any command mode, type "?" in the command mode.

```
Hostname#configure terminal
Hostname(config)# ?
   aaa                   Authentication, Authorization and Accounting
   access-list           Access List
   alarm                 Set alarm option of system
   arp                   Set a static ARP entry
   arp-security          To CPU arp security
   autosave              Auto save the startup configuration
   banner                Define a login banner
   cable-diagnostics     Cable Diagnostics on port
   change                Change user password
   check                 Check cpu utilization in interval time
   clear                 Command clear
.................................................... ......... ......
```

- Type a command followed by "?", and all sub-commands that can be executed in the current mode are displayed.

```
Hostname#show ?
   access-list           List access lists
   acl                   Acl
   acl-dot1x             Dot1x bind access-list
   acl-mac-chgvlan       Show acl interface ether
   acl-object            Show acl object
   acl-redir-port        Show acl interface ether
   arl                   Address translation item
   arp                   Command arp
   arp-security          To CPU arp security
..................................................... .....
```

- Type a character string followed by "?", and all the key words starting with the character string and their description are displayed.

```
Hostname#show a?
   access-list           List access lists
   acl                   Acl
   acl-dot1x             Dot1x bind access-list
   acl-mac-chgvlan       Show acl interface ether
   acl-object            Show acl object
   acl-redir-port        Show acl interface ether
   arl                   Address translation item
   arp                   Command arp
   arp-security          To CPU arp security
```

Command Line Error Messages

For all commands that are typed by users, the command line performs a syntax check. If the commands pass the syntax check, they are executed properly; otherwise, the system reports error messages to the users. The following table shows common error messages.

Table 1-3 Command Line Error Messages

Error Message	Error Cause
% Invalid input detected at '^' marker.	No command or key word is found, the parameter type is incorrect, or the parameter value is not within the valid range.
Type “*** ?” for a list of subcommands or % Incomplete command	The inputted command is incomplete.
Hostname#wh % Ambiguous command: wh % Please select: whoami who	The inputted character string is a fuzzy command.

History Commands

The command line interface provides a function that is similar to the Doskey function. The system automatically saves the user inputted commands into the history command cache. Then, users can invoke the history commands saved by the command line interface at any time and execute the command repeatedly, reducing unnecessary efforts in re-typing the commands. The command line interface saves up to 10 commands for each user that is connected to the device. Then, new commands overwrite old ones.

Table 1-4 Accessing History Commands of the Command Line Interface

To...	Press...	Execution Result
Access the previous history command	The up arrow key ↑ or Ctrl+P keys	If an earlier history command is available, it is displayed. If no earlier history command is available, an alarm sound is played.
Access the next history command	The down arrow key ↓ or Ctrl+P keys	If a later history command is available, it is displayed. If no later command is available, the commands are cleared, and an alarm sound is played.

NOTE

- If you want to access history commands by using the up and down arrow keys, when you telnet to the device in the Windows 98 or Windows NT OS, set Terminals >

Preferred Options > Simulation Options to VT-100/ANSI.

- History command display is based on the current command mode. For example, if you are in privileged mode, only history commands in privileged mode are displayed.

Editing Features

The command line interface provides basic command editing functions. It supports multi-line editing. Each line of command can contain up to 256 characters. The following table lists the basic editing functions that are provided by the shell subsystem for the command line interface.

Table 1-5 Basic Editing Functions

Key	Function
A common key	If the edit buffer is not full, the character is inserted to the position of the cursor, and the cursor moves to the right. If the edit buffer is full, an alarm sound is played.
The Backspace key	Deletes the character before the cursor and moves the cursor backward. If the cursor reaches the beginning of the command, an alarm sound is played.
The Delete key	Deletes the character behind the cursor. If the cursor reaches the end of the command, an alarm sound is played.
The left arrow key ← or Ctrl+B keys	Moves the cursor one characters to the left. If the cursor reaches the beginning of the command, an alarm sound is played.
The right arrow key → or Ctrl+F keys	Moves the cursor one characters to the right. If the cursor reaches the end of the command, an alarm sound is played.
The up and down arrow keys ↑↓	Display history commands.
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+U	Deletes all characters on the left of the cursor till the beginning of the command line.

Display Features

To facilitate users, the command line interface provides the following display features:

If the information to be displayed is more than one screen, the pause function is provided, and the prompt "---MORE---" is displayed at the lower left corner of the screen. At this time, the options displayed in the following table are available for users.

Table 1-6 Display Features

Key	**Function**
Space key, down arrow key ↓, or Ctrl-F	Display the next screen.
The up arrow key ↑ or Ctrl-B keys	Display the previous screen.
The Enter key, right arrow key → or equal key =	Scroll the displayed information one line down.
The left arrow key ← or the minus key -	Scroll the displayed information one line up.
Ctrl-H	Returns back to the topmost part of the displayed information.
Any other keys	Exits the display. Then, the information that has not been displayed will not be displayed.

2 System Login

2.1 Overview

The device supports the following system login modes:

- Logging into the device through the Console port for management and maintenance.
- Logging into the device through the AUX port for management and maintenance.
- Telnet (remote login). Users can manage and maintain the device remotely in this mode.
- Secure Shell (SSH). Through its encryption and authentication technology, SSH provides secure remote login management services for users.

2.2 System Login Function Configuration

Table 2-1 System Login Function Configuration List

Configuration Tasks	
Logging in to the device through the Console port	-
Logging in to the device through the AUX port	-
Configuring remote login through Telnet	Enable the Telnet service of the device.
	The device acts as a Telnet client for remote login.
Configuring remote login through SSH	Enable the SSH service of the device.
	The device acts as an SSH client for remote login.

NOTE

- For the related user configuration of Telnet and SSH remote login, refer to the login control and management manual.

2.2.1 Log in to Device via Console Port *-B -S -E -A*

To connect a terminal to the device through the Console port to configure the device, perform the following steps:

Step 1: Select a terminal.

The terminal can be a terminal with a standard RS-232 serial port or an ordinary PC, and the latter one is more frequently used. If the remote dial-up login mode is selected, two Modems are required.

Step 2: Connect the physical connection of the Console port.

Ensure that the terminal or the device that provides the Console port has been powered off, and then connect the RS-232 serial port of the terminal to the Console port of the device. The following figure shows the connection.

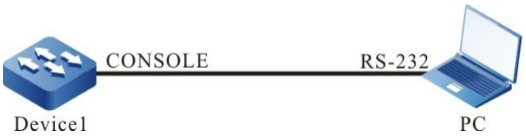


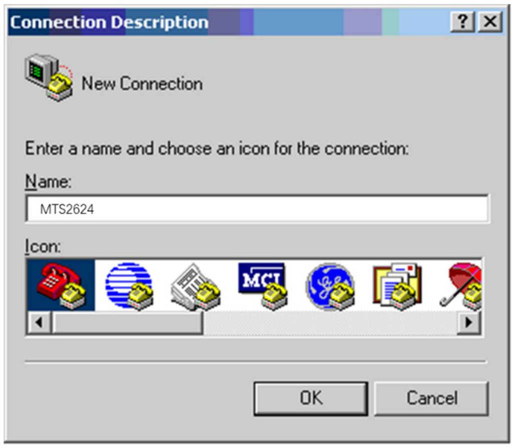
Figure 2-1 Connection for Login via the Console Port

Step 3: Configure the HyperTerminal.

After powering on the terminal, you need to set the communication parameters of the terminal, that is, baud rate of 9600 bps, 8 data bits, 1 stop bit, no parity check, and no data stream control. For a PC with the Windows XP or Windows NT OS, run the HyperTerminal program, and set the communication parameters of the serial port of the HyperTerminal according to the previously mentioned settings. The following takes the HyperTerminal in the Windows NT OS for example.

- Create a connection:

Input a connection name, and select a Windows icon for the connection.



New Connection

Enter a name and choose an icon for the connection:

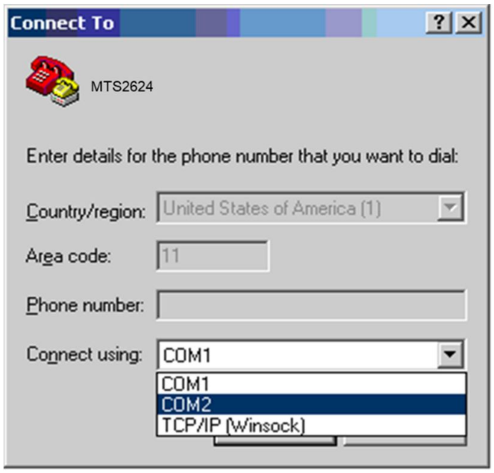
Name: MTS2624

Icon:

Figure 2-2 Creating a Connection

- Select a serial communication port:

According to the serial communication port that has been connected, select COM1 or COM2.



MTS2624

Enter details for the phone number that you want to dial:

Country/region: United States of America (1)

Area code: 11

Phone number:

Connect using: COM1

COM1
COM2
TCP/IP (Winsock)

Figure 2-3 Selecting a Serial Communication Port

- Configure parameters for the serial communication port:

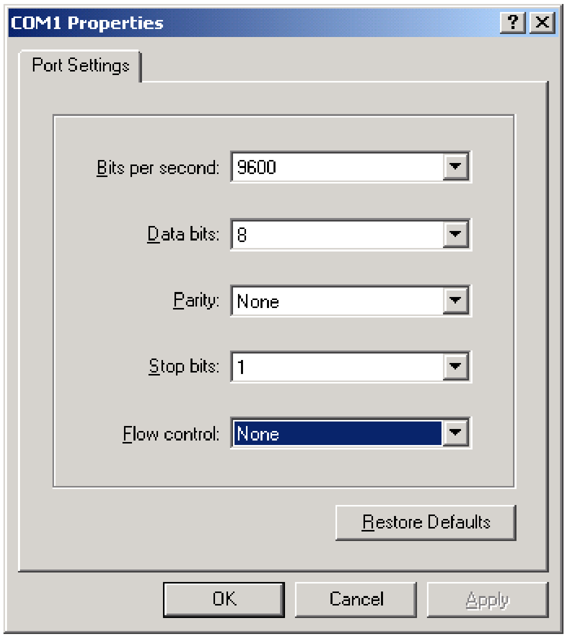
Baud rate: 9600 bps

Data bit: 8 bits

Parity check: None

Stop bit: 1 bit

Data stream control: None



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 2-4 Configuring Parameters for the Serial Communication Port

- Login success authentication:

After the device with the Console port is powered on, the startup information of the device is displayed on the terminal. After the startup is completed, the "Press any key to start the shell!" message is displayed. If login authentication is configured to be required, input the user name and password; otherwise, press any key to log in directly. After the login succeeds, the "Hostname>" prompt is displayed on the terminal. Then, you can configure the device.

2.2.2 Configure Remote Login via Telnet *-B -S -E -A*

Configuration Conditions

None

Enable Telnet service of Device

A user can log in to the device remotely through Telnet for management and maintenance. Before using the Telnet service, enable the Telnet service of the device. After the Telnet service of the device is enabled, the Telnet service port 23 is monitored.

Table 2-2 Enabling the Telnet Service of the Device

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the Telnet service of the device.	**telnet server enable**	Mandatory. By default, the Telnet service is enabled.

Take Device as Telnet Client for Remote Login

The user takes the device as a Telnet client to log in to the specified Telnet server for configuration and management.

Table 2-3 Taking the Device as a Telnet Client for Remote Login

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the Telnet client of the device.	**telnet client enable**	Optional. By default, the Telnet client is enabled.
Take the device as a Telnet client for remote login.	**telnet** [**vrf** *vrf-name*] { *hostname* | *remote-host* } [*port-number*] [**ipv4** | **ipv6**] [**source-interface** *interface-name*]	Mandatory.

NOTE

- The Telnet client can log in to a remote device only when the Telnet server function of the remote device is enabled, and the network between the Telnet client and the remote device is normal.

2.2.3 Configure Remote Login via SSH *-B -S -E -A*

Configuration Conditions

None

Enable the SSH Service of the Device

After the SSH server of a device is enabled, the device accepts the connection request initiated by the user from the SSHv1 or SSHv2 client. After the client passes the authentication, the client can access the device. After the SSH service of the device is enabled, the SSH service port 22 is monitored. If the **ip ssh server** command is used without parameter **sshv1-compatible**, it indicates that an SSH client can log in only through SSHv2.

Table 2-4 Enabling the SSH Service of the Device

Step	**Command**	**Description**
Enter the global configuration mode.	**config terminal**	-
Enable the SSH service of the device.	**ip ssh server** [**sshv1-compatible**]	Mandatory. By default, the SSH service is disabled.

Take the Device as an SSH Client for Remote Login

The device acts as an SSH client to log in to the specified SSH server remotely through the SSHv1 or SSHv2 protocol. During the login, a user name and a password are required for authentication from the SSH server.

Table 2-5 Taking an SSH Client for Remote Login

Step	Command	Description
Take the device as an SSH client for remote login.	**ssh version** { **1 | 2** } *remote-host port-number user* **auth-method 1** *password*	Mandatory.

NOTE

- The Telnet client can log in to a remote device only when the SSH service of the remote device is enabled, and the network between the SSH client and the remote device is normal.

2.2.4 System Login Monitoring and Maintaining *-B -S -E -A*

Table 2-6 System Login Monitoring and Maintaining

Command	Description
show fingerprint	Display the fingerprint information of the SSH public key.

2.3 Typical Configuration Example of System Login

2.3.1 Configure a Local Terminal to Telnet to the Device *-B -S -E -A*

Network Requirements

- A PC is used as a local terminal to log in to the device through Telnet.
- A route must be available between the PC and the device.

Network Topology

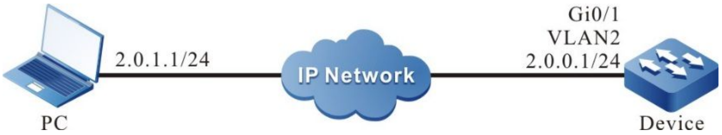


Figure 2-5 Network Topology for Configuring a Local Terminal to Telnet to the Device

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure the **enable** password.

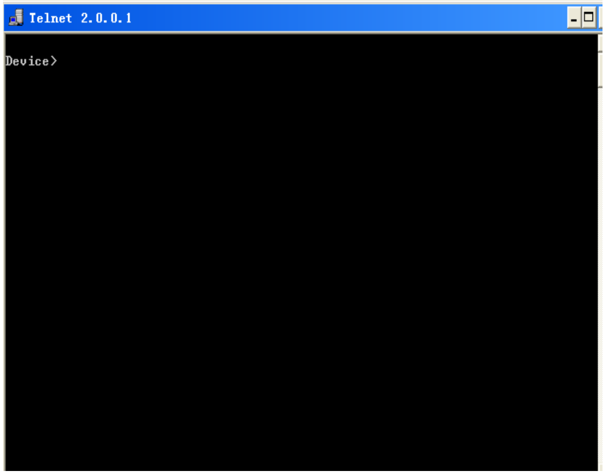
```
Device#configure terminal
Device(config)#enable password admin
```

Step 4: Telnet to the device.

#On the PC, run the Telnet program, and input the IP address of VLAN 2.

Step 5: Check the result.

#If the login succeeds, a window as shown in the following figure is displayed.



```
Device>
```

Figure 2-6 Window Displayed after Telnet Success

After logging in to the device successfully, input the correct **enable** password to obtain the required operation rights of the device. To log out of the device, input the **exit** command continuously.

NOTE

- If the "Too many clients or invalid access" message is displayed, it indicates that the number of login users has reached the maximum allowed number of login users of the device. In this case, wait a while and try to log in again.
- If the "%enable operation is locked by login-secure service" message is displayed, it indicates that the number of **enable** password input errors exceeds the number of continuous login authentication failures. If the number of **enable** password input errors reaches the number specified by the system, the system rejects the login connection request from the IP address during the specified time.
- If the "Password required, but none set" message is displayed, it indicates that no login password has been configured.

2.3.2 Configure a Local Device to Log in to a Remote Device via Telnet

-B -S -E -A

Network Requirements

- The local device Device1 acts as the Telnet client, while the remote device Device2 acts as the Telnet server.
- A route must be available between the two devices.
- The PC can normally log in to Device1.

Network Topology

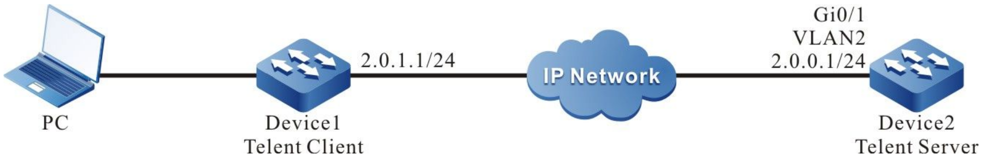


Figure 2-7 Network Topology for Configuring a Local Device to Telnet to a Remote Device

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Log in to Device1 through the PC. (Omitted)

Step 4: On Device1, run the following command to Telnet to Device2.

```
Device1#telnet 2.0.0.1
#Enter the shell screen of Device2.
Connect to 2.0.0.1 ...done
Device2>
```

After logging in to the Device2 successfully, input the correct **enable** password to obtain the required operation rights of the device. To log off the device, input the **exit** command continuously.

NOTE

- If the "Too many clients or invalid access" message is displayed, it indicates that the number of login users has reached the maximum allowed number of login users of the device. In this case, wait a while and try to log in again.
- If the "%enable operation is locked by login-secure service" message is displayed, it indicates that the number of **enable** password input errors exceeds the number of continuous login authentication failures. If the number of **enable** password input errors reaches the number specified by the system, the system rejects the login connection request from the IP address during the specified time.
- If the "Password required, but none set" message is displayed, it indicates that no login password has been configured.

2.3.3 Configure a Local Device to Log in to a Remote Device via SSH

-B -S -E -A

Network Requirements

- The local device Device1 acts as the SSH client, while the remote device Device2 acts as the SSH server.
- A route must be available between the two devices.
- The PC can normally log in to Device1.

Network Topology

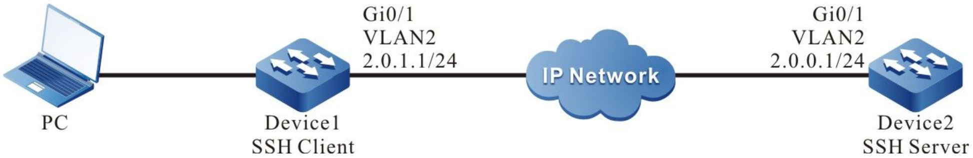


Figure 2-8 Network Topology for Configuring a Local Device to Log in to a Remote Device via SSH

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configures IP addresses for the ports. (Omitted)

Step 3: Configure a local user and the related properties.

#Configure the user name and password of Device2.

```
Device2#configure terminal
Device2(config)#user admin password 0 admin
```

Step 4: Enable the SSH server function of Device2.

```
Device2(config)#ip ssh server
```

Step 5: Set the login authentication mode to local authentication.

```
Device2(config)#line vty 0 15
Device2(config-line)#login local
Device2(config-line)#exit
```

Step 6: #On Device1, log in to Device2 through SSH.

#Configure Device1 to log in to Device2 through SSH.

```
Device1#ssh  version 2 2.0.0.1 22 admin auth-method 1 admin
The authenticity of host '2.0.0.1' can't be established
RSA key fingerprint is 7b:ed:cc:81:cf:12:36:6f:f7:ff:29:15:63:75:64:10.
Are you sure you want to continue connecting (yes/no)? yes
Device2>
```

Step 7: Check the result.

If the login succeeds, the shell screen of Device2 is displayed.

NOTE

- If the "Connection closed by foreign host" message is displayed, it indicates that the SSH service of the peer end is disabled, or the inputted user name or password is incorrect.
- The SSH server can be configured not to use authentication. If the SSH server does not use authentication, when a client logs in, a user can use any character string as the user name and password.

2.3.4 Configure a Device to Serve as SFTP Client *-B -S -E -A*

Network Requirements

- A PC is used as the SFTP server, a Device is used as the SFTP client; the server and device are connected via network.
- In SFTP server, set the user name with which the device log on to the FTP server to admin and the password to admin; place the file(s) to be downloaded under the SFTP server's directory.
- The device is used as the SFTP client to upload file(s) to/download file(s) from the SFTP server.

Network Topology

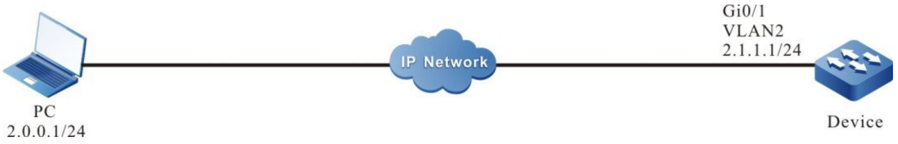


Figure 2-9 Networking Diagram - Configure a Device to Serve as SFTP Client

Configuration Steps

Step 1: Create a VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the SFTP server, place the file(s) to be downloaded under the SFTP server's directory. (omitted)

Step 3: Configure the Devices' IP addresses, so that the clients are connected to the server via network. (omitted)

Step 4: The Device is used as SFTP client to upload file(s) to/download file(s) from the SFTP server.

# Download a file from the SFTP server to the file system of the Device

```
Device#sftp get 2.0.0.1 22 admin admin sp8-g-6.6.7(46)-dbg.pck sp8-g-6.6.7(46)-dbg.pck
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes
```

```
Downloading###############################################################################
##############################################################OK!
```

# Upload the startup file under the Device's file system to the SFTP server

```
Device#sftp put 2.0.0.1 22 admin admin startup startup.txt

The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.

RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.

Are you sure you want to continue connecting (yes/no)? yes


Uploading#################################################################################
####################################################################################OK!
```

Step 5:   Check the result.

# Upon completion of the copying, the user can check the Device's file system to see whether the downloaded file exists or not; and check the SFTP server to see whether the uploaded file exists or not (omitted).

```
Device(config-fs)#dir

  size        date       time       name

--------      ------     ------    --------

101526     MAR-01-2015  01:17:18   logging

10147      MAR-26-2015  07:58:50   startup

10207      MAR-01-2015  01:17:54   history

11676148    MAR-26-2013  07:51:32  sp8-g-6.6.7(46)-dbg.pck

2048       JAN-10-2015  17:30:20   snmp             <DIR>
```

2.3.5 Configure a Device as SFTP Server   *-B -S -E -A*

Network Requirements

- The Device is used as SFTP server, the PC is used as SFTP client; the client and the server are connected via network.
- On the SFTP server Device, set the user name to admin and the password to admin, and use Device's file system directory as the SFTP server's root directory.
- Use the PC as SFTP client to upload file(s) to/download file(s) from the SFTP server Device.

Network Topology

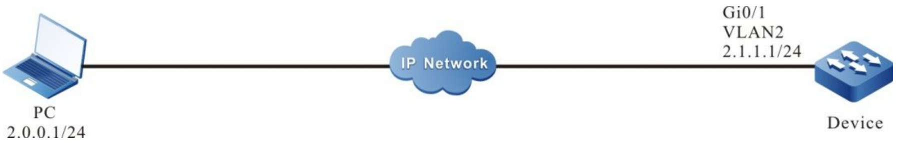


Figure 2-10 Networking Diagram - Configure a Device as SFTP Server

Configuration Steps

Step 1: Create a VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses, so that the PC is connected to the Device via network. (omitted)

Step 3: On the Device, enable SFTP service, configure authorized user' name and password.

# On the SFTP server Device, configure authorized user's name and password

```
Device#configure terminal
Device(config)#user admin password 0 admin
```

# Enable SSH service on the Device (SFTP is sub-module of SSH protocol)

```
Device(config)#ip ssh server
```

Step 4: Use the PC as SFTP client to upload a file to/download a file from the SFTP server Device.

# The following descriptions of relevant processes are based on Linux system

# Enter correct IP address and user name and password to log on to the SFTP server

```
[root@aas ~]# sftp admin@2.1.1.1
Connecting to 2.1.1.1...
admin@2.1.1.1's password:
sftp>
```

# Get the startup file from the SFTP server Device's file system

```
sftp> get startup startup
Fetching /flash/startup to startup
/flash/startup                                              100%   13KB  12.9KB/s   00:00
```

# Upon completion of the file copying process, relevant files can be found under the manipulated directory

```
sftp> ls
sp8-g-6.6.7(74)-dbg.pck   sp8-g-6.6.7(76)-dbg.pck   startup            tech              test_pc
sftp>
```

# Upload files from PC to the SFTP server Device's file system.

```
sftp> put sp8-g-6.6.7(76)-dbg.pck sp8-g-6.6.7(76)-dbg.pck
Uploading sp8-g-6.6.7(76)-dbg.pck to /flash/ sp8-g-6.6.7(76)-dbg.pck
```

```
sp8-g-6.6.7(76)-dbg.pck                                   100% 11424KB  16.0KB/s   00:00
```

# Upon completion of file uploading, corresponding files can be found in the Device's file system

```
Device(config-fs)#dir
  size       date       time     name
------------   ------     ------   --------
2048        JUN-30-2015  16:35:50   tech          <DIR>
10229        JUN-12-2015  14:31:22   history
101890        JUN-30-2015  17:46:40   logging
39755        JUN-30-2015  16:33:56   startup
740574        MAY-27-2014  18:55:14   web-Spl-1.1.243.rom
2048        JUN-27-2015  16:26:10   snmp          <DIR>
11698172       JUN-30-2015  10:36:18   sp8-g-6.6.7(76)-dbg.pck
```

3 System Control and Management

3.1 Overview

To enhance the operation security of the device, in user login or enable operation, the device provides multiple authentication management types (including AAA. Refer to the related sections and chapters in AAA configuration manual.) Only the user with the required operation rights can log in or perform the **enable** operation successfully.

To authorize different set of executable commands to different level of users, the device commands are divided into levels 0-15, and user levels are divided into levels 0-15. Among the levels, level 0 has the lowest rights while level 15 has the highest rights.

3.2 Login Control and Management Function Configuration

Table 3-1 Configuration List of Login Control and Management

Configuration Tasks	
Switch over between user levels.	Switch over between user levels.
Configure the command level.	Configure the command level.
Configure the **enable** password.	Configure the **enable** password.
Configure users and the related properties.	Configure auto commands.
	Configure no password authentication during login.
	Configure user passwords.
	Configure the user privilege level.
Configure line properties.	Enter the line configuration mode of the Console port.

Configuration Tasks	
	Enter the line configuration mode of the Telnet or SSH user.
	Configure the absolute time for the login user operation.
	Configure the privilege level of the login user.
	Configure users to automatically execute commands after login.
	Configure auto command execution options.
	Configure login user idle timeout time.
	Configure the line password.
	Configure the login authentication mode.
	Configure the line authorization mode.
	Configure the line accounting mode.
	Enable the Modem function of the Console port.
	Configure the user login timeout time.

3.2.1 Switch Over Between User Levels *-B -S -E -A*

If a user name and password of the corresponding level is configured, the user can run the **enable level (0-15)** command and then enter the correct password to enter the required user level. Meanwhile, the user has the execute permission of the user level and the lower levels.

If the current user level is higher than the user level that the user wants to enter, then no authentication is required, and the user directly enters the required user level. If the user level that the user wants to enter is higher than the current user level, authentication is required according to the current configuration, and the authentication mode is selected according to the configuration.

If the **enable** password of the corresponding level has been configured (by using the **enable password level** command), while the enable authentication of Authorization, Authentication and Accounting (AAA) is not configured or the AAA enable authentication is set to use the enable method, use the **enable** password for authentication.

If the **enable** password of the required level has not been configured, but the enable authentication method is set to use the local enable password for authentication, there are two cases:

a) In the case of a Telnet user, the login fails. If AAA has not been configured, the "% No password set" is prompted. If AAA has been configured, the "% Error in authentication" message is prompted.

b) For a Console port user, if AAA has been configured, try to use the enable password for authentication during the login. If the enable password has not been configured, use the none authentication method. That is, the login passes the authentication by default. If AAA has not been configured, the "% No password set" message is prompted, and the authentication fails.

If enable authentication succeeds, the user enters the specified user level and the user has execution permission of the level. To query the user level of the current user, run the **show privilege** command.

If the **aaa authentication enable default method** is configured and a related method list is used to enable authentication, then the related method is required for authentication, including:

a) If **aaa authentication enable default none** is configured, no password is required.

b) If **aaa authentication enable default line** is configured, and the line password is configured, use the password for authentication. Otherwise, the "% Error in authentication" message is prompted, and the authentication fails.

c) If **aaa authentication enable default radius** is configured, Remote Authentication Dial in User Service (RADIUS) authentication is used. Note that the enable authentication user names for RADIUS are fixed, that is, $enab+level$. Here "level" is a number in the range of 1-15, that is, the level that the user wants to enter. The RADIUS user names are fixed, therefore, during authentication, no user name is required. The user needs only to input the password. If passwords have been set for users of different levels on the RADIUS server, after inputting the correct password, the login succeeds; otherwise, the login fails. For example, in running the **enable 10** command, the fixed user name is $enab10$. If the user name exists on the RADIUS server, input the password corresponding to the user name, and then the authentication succeeds.

c) If **aaa authentication enable default tacacs** is configured, Terminal Access Controller Access Control System (TACACS) authentication is used. If the user name is displayed during login, keep the user name for login, and input the enable password of the user name. Otherwise, input a user name and the enable password of the user name. If the inputted user name exists in the TACACS server and the enable password of the TACACS has been set, the authentication succeeds; otherwise, the authentication fails.

NOTE

- The previously mentioned enable authentication methods can form a combination in use.

Configuration Conditions

None

Switch Over Between User Levels

If a user has the corresponding authority, the user can switch from the common user mode to the privileged user mode by switching over between user levels with a command. Then, the user has the authority of the user level. If a user runs the command in the privileged user mode, the user level switchover is performed according to the command parameter.

Table 3-2 Switching Over Between User Levels

Step	Command	Description
Switch over between user levels.	**enable** [*level-number*]	Mandatory. By default, the user level is level 15.

3.2.2 Configure the Command Level *-B -S -E -A*

Configuration Conditions

None

Configure the Command Level

In the application program, each shell command has a default level, which can be modified through the **privilege** command. A user can execute only the commands with the level equal to or smaller than the user level. For example, a user with the user level 12 can execute only the commands with the levels 0-12. In configuring the command level, you need to make use of command modes. You can modify the level of a single command or all commands in a specified command mode.

Table 3-3 Configuring the Command Level

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the command level.	**privilege** *privilege-mode* **level** *level-number* [**all** | **command** *command-line*]	Mandatory.

3.2.3 Configure the enable Password *-B -S -E -A*

Configuration Conditions

None

Configure the enable Password

The enable password is the password that is used by a level of users to enter the local level. If no level is specified in the enable command, the password is set as the enable password of level 15 by default.

Table 3-4 Configuring the enable Password

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the **enable** password.	**enable password** [**level** *level-number*] [**0**] *password*	Mandatory. By default, no enable password is configured.

3.2.4 Configure line Properties *-B -S -E -A*

The device supports up to one Console port user and 16 Telnet or SSH users to log in at the same time. Line commands can set different authentication and authorization properties for the login users.

Configuration Conditions

None

Enter Line Configuration Mode of Console Port

To configure the Console port properties, you need to enter the line configuration mode of the Console port.

Table 3-5 Entering the line Configuration Mode of the Console Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enters the line configuration mode of the Console port.	**line con 0**	Mandatory

Enter the line Configuration Mode of the Telnet or SSH User

To configure the Telnet or SSH properties, you need to enter the line configuration mode of Telnet of SSH.

Table 3-6 Entering the line Configuration Mode of the Telnet or SSH User

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Telnet or SSH user.	**line vty** { *vty-min-number* } [*vty-max-number*]	Mandatory

Configure Absolute Time for Login User Operation

The absolute time for the login user operation refer to the timeout time from the successful login of a user to the automatic exit of the user, in the unit of minute. If the absolute time is set to 0, it indicates that the time is not limited. By default, the time is 0. In addition, five seconds before the configured time expires, the following prompt message is displayed: Line timeout expired.

Table 3-7 Configuring the Absolute Time for the Login User Operation

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or Virtual Type Terminal (VTY).	**line** { **con 0 | vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configure the absolute time for the login user operation.	**absolute-timeout** *absolute-timeout-number*	Mandatory. By default, the absolute time is 0, that is, no time limit.

Configure Privilege Level of Login User

Configure the privilege level of the login user. The default privilege level is 1. A user can execute only the commands with the level equal to or smaller than the current level.

Table 3-8 Configuring the Privilege Level of the Login User

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0 | vty** *vty-min-number* [*vty-max-number*] }	Mandatory.
Configure the privilege level of the login user.	**privilege level** *level-number*	Mandatory. The privilege level is 1.

Configure Users to Automatically Execute Commands after Login

Configure the commands to be automatically executed after users successfully log in. By default, no command is to be automatically executed.

Table 3-9 Configuring the Commands to be Automatically Executed after Successful Login

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configure the commands to be automatically executed after successful login.	**autocommand** *command-line*	Mandatory

Configure Auto Command Execution Options

You can configure delay time for auto commands, and configure whether to disconnect the user connection after the commands are executed automatically. By default, the command execution is not delayed, and the user connection is disconnected after the commands are executed automatically.

The auto command execution options include delay and whether to disconnect the user connection after command execution.

Table 3-10 Configuring Auto Command Execution Options

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory.
Configure the auto command execution options.	**autocommand-option** { **nohangup** [**delay** *delay-time-number*] | **delay** *delay-time-number* [**nohangup**] }	Mandatory.

NOTE

- The **autocommand-option** command is valid only after the autocommand function is configured.

Configure Login User Idle Timeout Time

If the time in which login user does not perform any operation on the device is longer than the idle timeout time, the device make the current login user to log out. The default idle timeout exit time is 5 minutes. If the time is set to 0, then idle timeout does not take effect.

Table 3-11 Configuring the Idle Timeout Exit Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configuring the idle timeout exit time.	**exec-timeout** *exec-timeout-minute_number* [*exec-timeout-second_number*]	Mandatory The default idle timeout exit time is 5 minutes.

Configure the Line Password

Use 0 and 7 to indicate whether the line password is in plain text or cipher text. 0 indicates that the password is in plain text while 7 indicates that the password is in cipher text. In interaction mode, only plain-text password is allowed. That is, in this mode, parameter value 0 is used.

Table 3-12 Configuring the Line Password

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configure the line password.	**password 0** *password*	Mandatory

Configure the Login Authentication Mode

The device supports the following login authentication modes:

- Login authentication mode: Uses line password authentication.
- Login local authentication mode: Uses the local user database authentication.
- Login authentication mode: Uses the AAA authentication.
- No login indicates that no authentication is required for login. (If AAA is not configured, this mode can be used.)
- By default, the login authentication mode is used for Telnet, and the login local authentication mode is used for SSH.

Table 3-13 Configuring the Login Authentication Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configure the login authentication mode.	**login** [**local** | **authencation**]	Mandatory

Configure the Line Authorization Mode

If the AAA function has been configured, you can reference exec or commands for each line to give authorization. For details, refer to the *AAA Configuration Guide*.

Table 3-14 Configuring the Line Authorization Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configuring the authorization mode.	**authorization** { **exec** | **commands** *level* } { **default** | *word* }	Mandatory

NOTE

- The **authorization** command can be configured only after AAA is enabled.

Configure the Line Statistics Mode

If the AAA function has been configured, you can reference exec or commands for each line for accounting. For details, refer to the *AAA Configuration Guide*.

Table 3-15 Configuring the Accounting Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory
Configuring the accounting mode.	**accounting** { **exec** | { **commands** *level* } } { **default** | *word* }	Mandatory. For the accounting method of exec and commands, refer to the *AAA Configuration Guide*.

NOTE

- The **accounting** command can be configured only after AAA is enabled.

Enable the Modem Function of the Console Port

The Console port of the device provides the functions of the AUX port. Therefore, you can enable the Modem function of the Console port to support remote dial-up login.

Table 3-16 Enabling the Modem Function of the Console Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Entering the line configuration mode of the console port.	**line con 0**	Mandatory
Enable the Modem function of the Console port.	**Modem auto-detection**	Mandatory. By default, the Modem function of the Console port is disabled.

Configure the User Login Timeout Time

During login, if the wait time for the user to input the user name or password times out, the system prompts that the login fails. By default, the login timeout time is 30 seconds. To modify the wait timeout time, use this function.

Table 3-17 Configuring the User Login Wait Timeout Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the line configuration mode of the Console port or VTY.	**line** { **con 0** | **vty** *vty-min-number* [*vty-max-number*] }	Mandatory.
Configure the user login wait timeout time.	**timeout login respond** *respond-time-value*	Mandatory. By default, the wait time for the user to input the user name or password is 30 seconds.

3.2.5 System Control and Management Monitoring and Maintaining *-B -S -E -A*

Table 3-18 System Control and Management Monitoring and Maintaining

Command	Description
clear line { **con** *con-number* | **vty** *vty-number* }	Clear a terminal service.
show privilege	View the privilege level of the current user.
show users	Display the configured user information.

4 FTP, FTPS, TFTP and SFTP

4.1 Overview

File Transfer Protocol (FTP) is used between a server and a client to transmit files. It improves file sharing, and provides an efficient and reliable data transmission mode between the user and remote computer. The FTP protocol usually uses TCP port 20 and 21 for transmission. Port 20 transmits data in active mode, and port 21 transmits control messages.

Similar to most Internet services, FTP uses the client/server communication mechanism. To connect to an FTP server, usually you are required to have the authorized account of the FTP server. On the Internet, a large number of FTP servers are anonymous FTP servers, which aim at provide file copying services to the public. For this type of FTP server, users need not register with the server or obtain authorization from the FTP servers.

FTP supports two types of file transmission modes:

- ASCII transmission mode, in which text files are transmitted.
- Binary transmission mode, in which program files are transmitted.

If the device acts as an FTP client, only the binary transmission mode is supported. If the device acts as an FTP server, both transmission modes are supported.

FTP supports two working modes:

- Active mode: An FTP client first sets up a connection with an FTP server through the TCP21 port and sends commands through this channel. If the FTP client wants to receive data, it sends the PORT command through this channel. The PORT command contains through which port the client receives data. Then the FTP server connects its TCP20 port to the specified port of the FTP client to transmit data. The FTP server must set up a new connection with the FTP client to transmit data.
- Passive mode: The method of setting up the control channel in passive mode is similar to that in active mode. However, after the connection is set up, the PASV command instead of the PORT command is sent. After the FTP server receives the PASV command, it opens a high end port (with the port number larger than 1024) and inform the client to transmit data through this port. The FTP client connects to the port of the FTP server, and then the FTP server transmits data through this port.

Many Intranet clients cannot log in to the FTP server in active mode, because the server fails to set up a new connection with an Intranet client.

When the device acts as an FTP client, it sets up a data connection in active mode.

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol which is based on the User Datagram Protocol (UDP). It transmits data through UDP port 69. The protocol is designed for transmission of small files; therefore, it does not have as many functions as the FTP protocol. It does not support list of directories or authentication. The device only implements the functions of the TFTP client.

4.1.1 Configure an FTP Server *-B -S -E -A*

Configuration Conditions

None

Configure the Functions of an FTP Server

Before configuring the device as the FTP server, first enable the FTP server function. Then, the FTP client can access the FTP server. For security sake, the device provides the FTP service only to authorized users, and it limits the maximum allowed number of concurrent login users.

Table 4–1 Configuring the Functions of an FTP Server

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the FTP server function.	**ftp enable**	Mandatory. By default, the FTP server function is disabled.
Configure the authorized user name and password.	**user** *username* **password 0** *password*	Mandatory. By default, the authorized user name and password are not configured. For details of the command, refer to the related sections in "System Control and Management".
Configure the FTP service listening port number	**ftp listen-port** [*port-num*]	Optional By default, the FTP service listening port number is 21.
Configure the maximum allowed number of concurrent login users.	**ftp max-user-num** *user-num*	Optional. By default, the maximum allowed number of concurrent login users is 1.
Configure the connection timeout time.	**ftp timeout** *time*	Optional.

Step	Command	Description
		By default, the connection timeout time is 300 seconds.

4.1.2 Configure an FTP Client *-B -S -E -A*

Configuration Conditions

None

Configure the Functions of an FTP Client

On the device, when you use the **copy** command to copy files (Refer to the related sections in "File System Management") or use the **sysupdate** command to upgrade the software version (Refer to the related sections in "Software Upgrade"), the device can be triggered to act as the FTP client and set up a connection with the remote FTP server.

The connection between an FTP client and an FTP server uses the address of the outgoing interface of the route to the FTP server as the source address by default. Users can also use the **ip ftp source-address** or **ip ftp source-interface** commands to specify the FTP client source address or source interface.

Table 4-2 Configuring the Functions of an FTP Client

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the source address of the FTP client.	**ip ftp** { **source-interface** *interface-name* | **source-address** *ip-address* }	Optional. By default, the FTP client uses the address of the outgoing interface of the route to the FTP server as its source address to communicate with the FTP server.
Exit to the privilege user mode.	**exit**	-
Enter the file system configuration mode.	**filesystem**	-
Copy files.	**copy** { *src-parameter* } { *dest-parameter* }	Optional. Use this command to download files from or upload files to the FTP

Step	Command	Description
		server. For details of the command, refer to the related section in "File System Management".
Exit to the privilege user mode.	**exit**	-
Upgrade the software version.	**sysupdate { image | monitor } mpu** [**vrf** *vrf-name*] *dest-ip-address filename* **ftp** *ftp-username ftp-password* [**reload**]	Optional. Use this command to upgrade image and monitor programs from the FTP server via the device interface. For details of the command, refer to the related section in "Software Upgrade".

NOTE

- For the security sake, some networks may restrict the communication between the address of the outgoing interface of the route from the device to the FTP server and the FTP server, but the other service interface addresses are available. In this case, users can use the **ip ftp source-address** or **ip ftp source-interface** commands to specify the FTP client source address or source interface.

4.1.3 Configure a TFTP Client *-B -S -E -A*

Configuration Conditions

None

Configure the Functions of a TFTP Client

On the device, when you use the **copy** command to copy files (Refer to the related sections in "File System Management") or use the **sysupdate** command to upgrade the software version (Refer to the related sections in "Software Upgrade"), the device can be triggered to act as the TFTP client and set up a connection with the remote TFTP server.

The connection between a TFTP client and a TFTP server uses the address of the outgoing interface of the route to the TFTP server as the source address by default. Users can also use the **ip tftp source-address** or **ip tftp source-interface** commands to specify the TFTP client source address or source interface.

Table 4-3 Configuring the Functions of a TFTP Client

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the source address of the TFTP client.	**ip tftp** { **source-interface** *interface-name* | **source-address** *ip-address* }	
Exit to the privilege user mode.	**exit**	-
Enter the file system configuration mode.	**filesystem**	-
Copy files.	**copy** { *src-parameter* } { *dest-parameter* }	Optional. By default, files are not copied. Use this command to download files from or upload files to the FTP server. For details of the command, refer to the related sections in "File System Management".
Exit to the privilege user mode.	**exit**	-
Upgrade the software version.	**sysupdate { image | monitor } mpu** [**vrf** *vrf-name*] *dest-ip-address filename* [**reload**]	Optional Use this command to upgrade image and monitor programs from the TFTP server via the device interface. For details about the commands, refer to the related section in the software upgrade manual.

NOTE

- For the security sake, some networks may restrict the communication between the address of the outgoing interface of the route from the device to the TFTP server and the TFTP server, but the other service interface addresses are available. In this case, users can use the **ip tftp source-address** or **ip tftp source-interface** commands to

	specify the TFTP client source address or source interface.	

4.1.4 Configure TFTP Server *-B -S -E -A*

Configuration Conditions

None

Configure TFTP Server Function

When configuring a Device as the TFTP server, TFTP server function has to be enabled first so that the TFTP client can access the server.

Table 4–4 Configure TFTP Server Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable TFTP server function	**tftp enable**	Required By default, the TFTP server function is disabled

4.1.5 Configure SFTP Server *-B -S -E -A*

Configuration Conditions

None

Configure SFTP Server Function

When configuring a Device as the SFTP server, SFTP server function has to be enabled first so that the SFTP client can access the server. As SFTP is a sub-function subordinated to SSH, the configurations for enabling the SFTP service are identical to those for enabling SSH remote login service.

Table 4–5 Configure SFTP Server Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enable SFTP server function	**ip ssh server [sshv1-compatible] [listen-port]**	Required By default, the SFTP server function is disabled

4.1.6 Configure SFTP Client *-B -S -E -A*

Configuration Conditions

None

Configure SFTP Client Function

The Device as an SFTP client connects to the SFTP server, downloading file(s) from the SFTP server or uploading file(s) to the SFTP server.

Table 4–6 Configure SFTP Client Function

Steps	Command	Description
Configure the Device as an SFTP client to upload file(s) to or download file(s) from the SFTP server	**sftp { get | put } [vrf vrf-name] host-ip-address port-number [source-interface interface-name] user password src-filename dest-filename [compress]**	Optional

4.1.7 FTP and TFTP Monitoring and Maintaining *-B -S -E -A*

None

4.2 FTP and TFTP Function Configuration

Table 4-7 FTP and TFTP Function Configuration List

Configuration Tasks	
Configure an FTP server.	Configure the functions of an FTP server.
Configure an FTP client.	Configure the functions of an FTP client.

Configuration Tasks	
Configure a TFTP client.	Configure the functions of a TFTP client.

4.2.1 Configure a Device as an FTP Client *-B -S -E -A*

Network Requirements

- A PC acts as an FTP server, and Device acts as an FTP client. The network between the server and the device is normal.
- On the FTP server, the user name for a device to log in to the FTP server is admin, and the password is admin. The files to be downloaded are placed in the FTP server directory.
- The device acts as the FTP client to upload files to and download files from the FTP server.

Network Topology

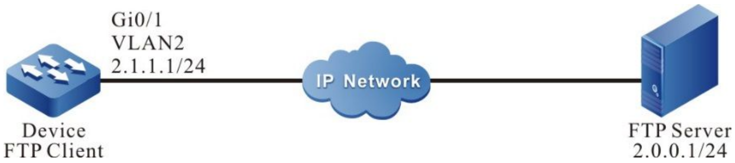


Figure 4-1 Networking for Configuring a Device as an FTP Client

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure an FTP server, and place the files to be downloaded in the FTP server directory. (Omitted)

Step 3: Configure the IP addresses of the devices so that the network between the client and the server is normal. (Omitted)

Step 4: Device acts as the FTP client to upload files to and download files from the FTP server. (Omitted)

#In the file system mode of the Device, copy one file from the FTP server to the file system of Device.

```
Device#filesystem
Device(config-fs)#copy ftp 2.0.0.1 admin admin sp4-g-6.5.0(41).pck file-system  sp4-g-6.5.0(41).pck
Device (config-fs)#exit
```

#In the file system mode of Device, copy the startup file of Device into the FTP server.

```
Device#filesystem
Device(config-fs)#copy file-system startup ftp 2.0.0.1 admin admin startup.txt
```

Step 5: Check the result.

#After the copy process is completed, check whether the downloaded file exists in the file system of Device. In the FTP server, check whether the uploaded file exists. (Omitted)

```
Device(config-fs)#dir
  size         date       time      name
--------       ------     ------    --------
101526     MAR-01-2013  01:17:18   logging
10147      MAR-26-2013  07:58:50   startup
10207      MAR-01-2013  01:17:54   history
1372       MAR-23-2013  08:18:38   devInfo
6598624    MAR-26-2013  07:51:32   sp4-g-6.5.0(41).pck
1024       JAN-10-2013  17:30:20   snmp              <DIR>
0          JAN-31-2013  14:29:50   syslog
736512     MAR-27-2013  10:30:48   web-Spl-1.1.168.rom
```

NOTE

- If the "FTP: Ctrl socket connect error(0x3c): Operation timed out" message is printed, it indicates that the server cannot be reached, and the cause may be that the route is not available or the server has not been started.
- If the "Downloading##OK!" message is printed, it indicates that the file is copied successfully.

4.2.2 Configure a Device as an FTP Server *-B -S -E -A*

Network Requirements

- Device1 acts as an FTP server, while PC and Device2 act as FTP clients. The network between the client and the server is normal.
- On the FTP server Device1, the user name is admin, and the password is admin. The file system directory of Device1 acts as the root directory of the FTP server.
- PC and Device2 act as the FTP client to upload files to and download files from the FTP server Device1.

Network Topology

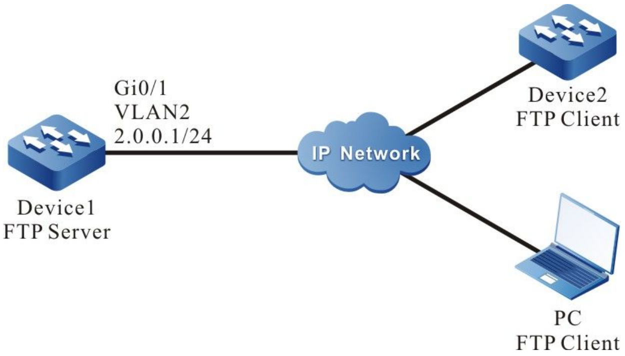


Figure 4–2 Networking in Which a Device Acts as an FTP Server

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure the IP addresses of the interfaces so that the network between the PC, Device 2, and Device 1 are normal. (Omitted)

Step 3: On Device1, enable the FTP service, and configure the authorized user name and password.

#On Device1, enable the FTP service, and configure the authorized user name and password.

```
Device1#configure terminal
Device1(config)#user admin password 0 admin
```

#On Device1, enable the FTP service.

```
Device1(config)#ftp enable
```

#On Device1, set the maximum number of concurrent users to 2.

```
Device1(config)#ftp max-user-num 2
```

Step 4: Check the result.

#Check whether the FTP service function is enabled on Device1.

```
Device#show ip sockets
Active Internet connections (including servers)
PCB      Proto Recv-Q Send-Q  Local Address         Foreign Address       vrf       (state)
-------- ----- ------ ------  --------------------- --------------------- -------    -------
27cf8a4  TCP       0      0  0.0.0.0.80            0.0.0.0               all       LISTEN
27ce0a4  TCP       0      0  130.255.104.43.22      130.255.98.2.3590     global    ESTABLISHED
27d0be4  TCP       0      0  0.0.0.0.21            0.0.0.0               all       LISTEN
27d0824  TCP       0      0  127.0.0.1.2622         127.0.0.1.1026        global    ESTABLISHED
```

If the FTP service function has enabled, you can find that port 21 is in the listen state.

Step 5: Use Device2 as an FTP client to copy a startup file from FTP server Device1 to Device2.

```
Device2#filesystem
Device2(config-fs)#copy ftp 2.0.0.1 admin admin startup file-system startup
```

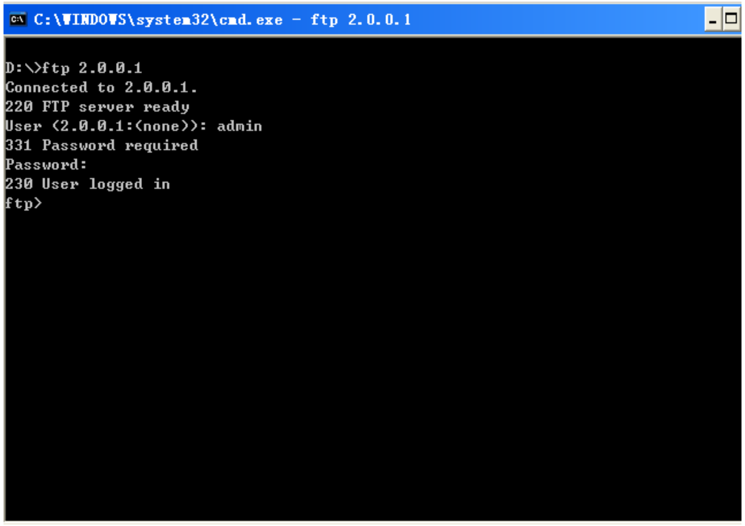
Step 6: Use PC as an FTP client to copy a startup file from FTP server Device1 to PC.

#In the following part, the Windows DOS screens are taken as an example to illustrate the process.

#In the Windows DOS screen, input the correct IP address, user name, and password to log in to the FTP server.

```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
```

ftp>

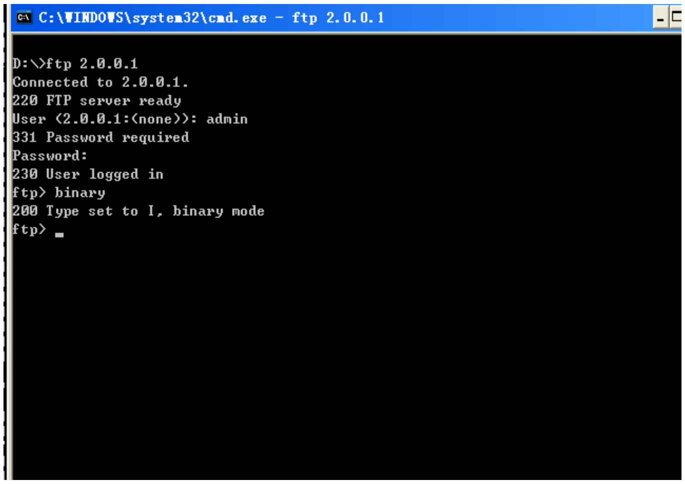


```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp>
```

Figure 4-3 Networking of the Device as the FTP Server

#Configure the PC and FTP server to transmit data in binary mode.

ftp>binary

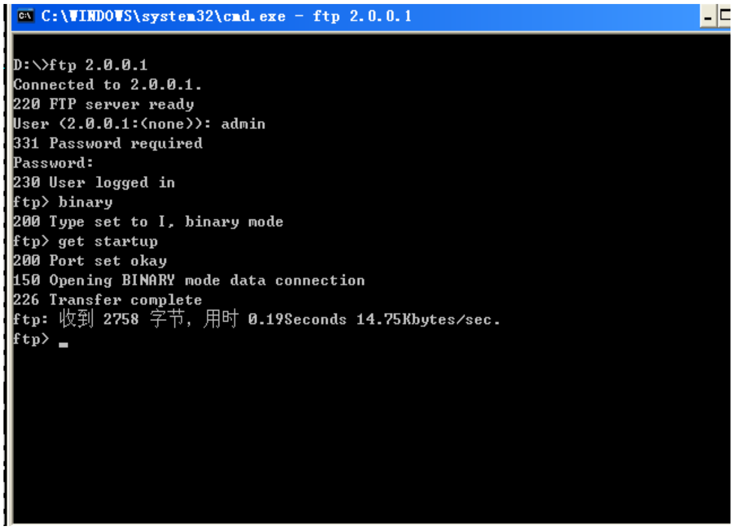


```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp> binary
200 Type set to I, binary mode
ftp> _
```

Figure 4-4 Configuring the PC and FTP Server to Transmit Data in Binary Mode

#Obtain the startup file in the file system of the FTP server Device1.

ftp>get startup



```
C:\WINDOWS\system32\cmd.exe - ftp 2.0.0.1

D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp> binary
200 Type set to I, binary mode
ftp> get startup
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 收到 2758 字节，用时 0.19Seconds 14.75Kbytes/sec.
ftp> _
```

Figure 4-5 Copying a Configuration File from the FTP Server

After the file copy process is completed, the file is available in the specified Windows directory.

NOTE

- If the "421 Session limit reached, closing control connection" message is printed, it indicates that the number of connections has exceeds the maximum number allowed by the server.
- When you use a device to copy a file, if the " Ctrl socket connect error(0x3c): Operation timed out" message is printed, the cause may be that the server function is not enabled, or the route between the server and the client is not reachable.
- When you connect the FTP server through the FTP client PC, if the " connect :Unknown error number" is printed, the cause may be that the server function is not enabled, or the route between the server and the client is not reachable.

4.2.3 Configure a Device as a TFTP Client *-B -S -E -A*

Network Requirements

- A PC acts as a TFTP server, and Device acts as a TFTP client. The network between the server and the device is normal. The files to be downloaded are placed in the TFTP server directory.
- The device acts as the TFTP client to upload files to and download files from the TFTP server.

Network Topology

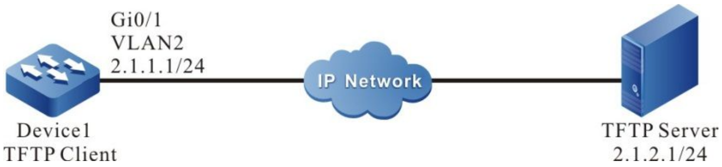


Figure 4-6 Networking for Configuring a Device as a TFTP Client

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure the IP addresses of the interfaces so that the network between the client and the server is normal. (Omitted)

Step 3: Enable the TFTP server function on PC, and place the files to be downloaded in the TFTP server directory. (Omitted)

Step 4: Device acts as the TFTP client to upload files to and download files from the TFTP server.

#On Device, copy a file from the TFTP server to the file system of Device.

```
Device#filesystem
Device(config-fs)#copy tftp 2.1.2.1 sp4-g-6.5.0(41).pck file-system sp4-g-6.5.0(41).pck
Device(config-fs)#exit
```

#On Device, copy the startup file from Device to the TFTP server.

```
Device#filesystem
Device(config-fs)#copy startup-config tftp 2.1.2.1 startup.txt
```

Step 5: Check the result.

After the copy process is completed, check whether the downloaded file exists in the file system of Device. In the TFTP server, check whether the uploaded file exists. (Omitted)

```
Device(config-fs)#dir
  size         date       time       name
--------       ------     ------    --------
102227     MAR-01-2013  05:24:32   logging
10147      MAR-26-2013  07:58:50   startup
10202      MAR-01-2013  05:26:46   history
6598624    MAR-26-2013  07:51:32   sp4-g-6.5.0(41).pck
1024       JAN-10-2013  17:30:20   snmp               <DIR>
0          JAN-31-2013  14:29:50   syslog
736512     MAR-27-2013  10:30:48   web-Spl-1.1.168.rom
```

NOTE

- If the "Downloading####OK!" message is printed, it indicates that the file copy is successful. The message shows the file size, which is determined by the actual file size.
- When you use a device to copy a file, if the " Failed! ErrorNum: 0x41, ErrorType: Host unreach." message is printed, the cause may be that the TFTP server function is not

enabled, or the route between the server and the client is not reachable.

4.2.4 Configure a Device as an SFTP Client *-B -S -E -A*

Network Requirements

- A PC is used as the SFTP server, a Device is used as the SFTP client; the server and device are connected via network.
- In SFTP server, set the user name with which the Device log on to the SFTP server to admin and the password to admin; place the file(s) to be downloaded under the SFTP server's directory.
- The Device is used as the SFTP client to upload file(s) to/download file(s) from the SFTP server.

Network Topology

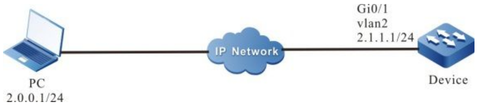


Figure 4–7 Networking Diagram - Configure a Device as an SFTP Client

Configuration Steps

Step 1: Configure the SFTP server, place the file(s) to be downloaded under the SFTP server's directory. (omitted)

Step 2: Configure the Devices' IP addresses, so that the clients are connected to the server via network. (omitted)

Step 3: The Device is used as SFTP client to upload file(s) to/download file(s) from the SFTP server.

# Download a file from the SFTP server to the file system of the Device

```
Device#sftp get 2.0.0.1 22 admin admin sp8-g-6.6.7(46)-dbg.pck sp8-g-6.6.7(46)-dbg.pck

The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.

RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.

Are you sure you want to continue connecting (yes/no)? yes

Downloading###################################################################################################
##############################################################################
```

# Upload the startup file under the Device's file system to the SFTP server

```
Device#sftp put 2.0.0.1 22 admin admin startup startup.txt

The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.

RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.

Are you sure you want to continue connecting (yes/no)? yes

Uploading#####################################################################################################
#########################################################################################################
```

Step 4: Check the result.

# Upon completion of the copying, the user can check the Device's file system to see whether the downloaded file exists or not; and check the SFTP server to see whether the uploaded file exists or not (omitted).

```
Device(config-fs)#dir
  size        date       time      name
--------      ------     ------    --------
101526    MAR-01-2015  01:17:18   logging
10147     MAR-26-2015  07:58:50   startup
10207     MAR-01-2015  01:17:54   history
11676148    MAR-26-2013  07:51:32  sp8-g-6.6.7(46)-dbg.pck
2048      JAN-10-2015  17:30:20   snmp            <DIR>
```

4.2.5 Configure a Device as an SFTP Server -B -S -E -A

Network Requirements

- The Device is used as SFTP server, the PC is used as SFTP client; the client and the server are connected via network.
- On the SFTP server Device, set the user name to admin and the password to admin, and use Device's file system directory as the SFTP server's root directory.
- Use the PC as SFTP client to upload file(s) to/download file(s) from the SFTP server Device.

Network Topology

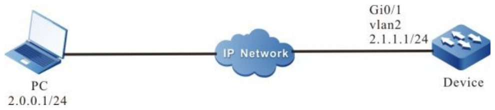


Figure 4–8 Networking Diagram - Configure a Device as an SFTP Server

Configuration Steps

Step 1: Configure the interfaces' IP addresses, so that the PC is connected to the Device via network. (omitted)

Step 2: On the Device, enable SFTP service, configure authorized user' name and password.

# On the SFTP server Device, configure authorized user's name and password

```
Device#configure terminal
Device(config)#user admin password 0 admin
```

# Enable SSH service on the Device (SFTP is sub-module of SSH protocol)

```
Device(config)#ip ssh server
```

Step 3: Use the PC as SFTP client to upload a file to/download a file from the SFTP server Device.

# The following descriptions of relevant processes are based on Linux system

# Enter correct IP address and user name and password to log on to the SFTP server

```
[root@aas ~]# sftp admin@2.1.1.1

Connecting to 2.1.1.1...

admin@2.1.1.1's password:

sftp>
```

# Get the startup file from the SFTP server Device's file system

```
sftp> get startup startup

Fetching /flash/startup to startup

/flash/startup                                              100%   13KB  12.9KB/s   00:00
```

# Upon completion of the file copying process, relevant files can be found under the manipulated directory

```
sftp> ls

sp8-g-6.6.7(74)-dbg.pck   sp8-g-6.6.7(76)-dbg.pck   startup              tech                  test_pc

sftp>
```

# Upload files from PC to the SFTP server Device's file system.

```
sftp> put sp8-g-6.6.7(76)-dbg.pck sp8-g-6.6.7(76)-dbg.pck

Uploading sp8-g-6.6.7(76)-dbg.pck to /flash/ sp8-g-6.6.7(76)-dbg.pck

sp8-g-6.6.7(76)-dbg.pck                                         100% 11424KB  16.0KB/s   00:00
```

# Upon completion of file uploading, corresponding files can be found in the Device's file system

```
Device(config-fs)#dir

  size         date         time      name

------------     ------       ------    --------

2048           JUN-30-2015  16:35:50   tech              <DIR>

10229           JUN-12-2015  14:31:22   history

101890          JUN-30-2015  17:46:40   logging

39755           JUN-30-2015  16:33:56   startup

740574          MAY-27-2014  18:55:14   web-Spl-1.1.243.rom

2048           JUN-27-2015  16:26:10   snmp              <DIR>

11698172        JUN-30-2015  10:36:18   sp8-g-6.6.7(76)-dbg.pck
```

4.2.6 Configure a Device as an FTPS Client *-B -S -E -A*

Network Requirements

- The PC is used as FTP Server, the Device is used as FTP Client; the Server is connected to the Client via network.
- A secure data channel is established between the FTP Server and the FTP Client to safeguard data transmission.
- FTP Client can upload file(s) to and download file(s) from the FTP Server.

Network Topology

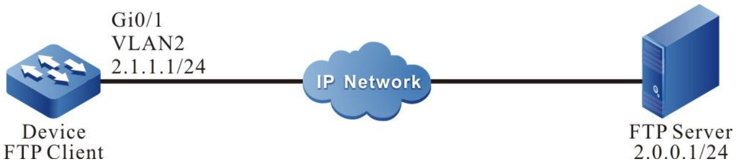
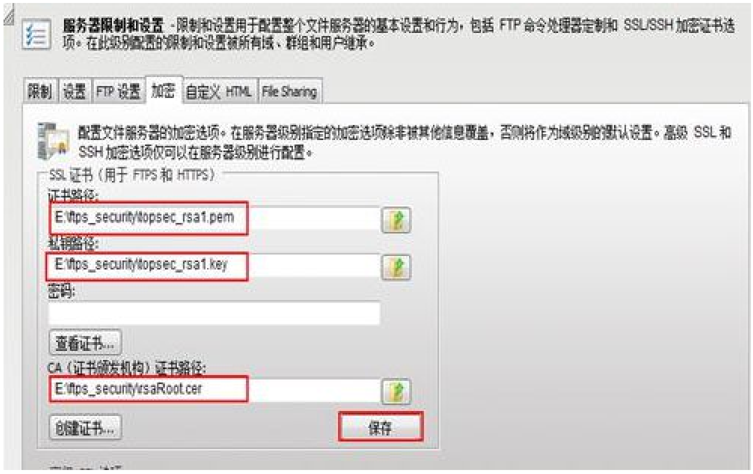


Figure 4–9 Networking Diagram - Configure a Device as an FTPS Client

Configuration Steps

Step 1: Configure IPv4 addresses for the ports. (omitted)

Step 2: Install certificate on the FTP Server and set up FTP user certificate path, private key path, CA certificate path:



服务器限制和设置 -限制和设置用于配置整个文件服务器的基本设置和行为，包括 FTP 命令处理器定制和 SSL/SSH 加密证书选项。在此级别配置的限制和设置被所有域、群组和用户继承。

配置文件服务器的加密选项。在服务器级别指定的加密选项除非被其他信息覆盖，否则将作为域级别的默认设置。高级 SSL 和 SSH 加密选项仅可以在服务器级别进行配置。

SSL 证书（用于 FTPS 和 HTTPS）

证书路径: E:\ftps_security\topsec_rsa1.pem

私钥路径: E:\ftps_security\topsec_rsa1.key

密码:

CA（证书颁发机构）证书路径: E:\ftps_security\rsaRoot.cer

Step 3: Import FTP CA certificate, user certificate, private key to the FTP Client.

# Create a domain test on the Device:

```
Device#configure terminal
Device(config)#crypto ca identity test
Device(ca-identity)#exit
```

# Bind ftp to the domain test:

```
Device(config)#ip ftp secure-identity test
```

# Open the CA certificate (rsaRoot.cer) with Notepad, copy the content in the certificate, enter crypto ca import certificate to test on shell, follow the prompts to import the certificate to the Device domain test:

```
Device(config)#crypto ca import certificate to test
% Input the certificate data, press <Enter> twice to finish:
-----BEGIN CERTIFICATE-----
MIIDBzCCAnCgAwIBAgIITpXH17Hj/AswDQYJKoZIhvcNAQEFBQAwYjELMAkGA1UE
BhMCQ04xEDAOBgNVBAgMB0JFSUpJTkcxDjAMBgNVBAoMBUNJRUNDMQ8wDQYDVQQL
DAZHRkEgQ0ExIDAeBgNVBAMMF01pbmlDQSBGcmVCU0QgUm9vdCBDZXJ0MB4XDTA5
MDgwMzA2MDY1MloXDTE5MDgwMzA2MDY1MlowYjELMAkGA1UEBhMCQ04xEDAOBgNV
BAgMB0JFSUpJTkcxDjAMBgNVBAoMBUNJRUNDMQ8wDQYDVQQLDAZHRkEgQ0ExIDAe
BgNVBAMMF01pbmlDQSBGcmVCU0QgUm9vdCBDZXJ0MIGeMA0GCSqGSIb3DQEBAQUA
A4GMADCBiAKBgHXZMtpxzH8p0uUt6QomUhuJNcy9iyYhoJVx4I3T6kpmx9cdzapM
RoKUa9eB/jCzhgctQc7ZDuKP+gafHWgZtbzwwSVksVsNmFqBivixveGx9dCrtequ
+vDiXVyDVPSNDDTmamMGYyCb0N7aSOzdgv6BYyQKyy/Y0FK6/v/v4NUxAgMBAAGj
gcYwgcMwPQYDVR0fBDYwNDAyoDCgLoYsaHR0cDovLzE2OC4xNjguMTcuNDY6OTAw
MC9nZmEvY3JsL2dmYWFwcC5jcmwwSAYDVR0gBEEwPzA9BggrBgEEAYcrMjAxMC8G
CCsGAQUFBwIBFiNodHRwOi8vd3d3LmdmYXBraS5jb20uY24vcG9saWN5LmRvYzAL
BgNVHQ8EBAMCAuQwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUhnY8uZXbE2iX1mXO
ipvfuDUgAeswDQYJKoZIhvcNAQEFBQADgYEAcNPdTE+YpfOQn8lW1oF7TkGJ/Vzd
c0O5UUB+jPhYkj+fXUX8WyxabOxgl3u+7DJ/3gHw1rO8ZcDO94Wz+nBsile5tFv7
/bHz0yqJVoUJMIaWOdmLXJj5fI5GeBCprzLM88RJCv6LBHfg4ThOC4Ds80Ssive1
eAod+7kbmVPOZg8=
-----END CERTIFICATE-----

% Input the private key data, press <Enter> twice after data to finish or press <Enter> without data to ignore:

% The Root CA Certificate has the following attributes:
  Serial Number: 4e95c7d7b1e3fc0b
  Subject: C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
  Issuer : C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
  Validity
    Start date: 2009-08-03 06:06:52
    End   date: 2019-08-03 06:06:52
  Usage: General
  Fingerprint(sm3) :18d39e4c50c9ad8b11446ac7ac1736f853ac92e769994b98233b48787562429c
  Fingerprint(sha1):ab3559e26384539ffcac3c76b5a5e7a1f7073dfb

% Do you accept this root ca-certificate[yes]/[no]:
% Please answer 'yes' or 'no'.
% Do you accept this root ca-certificate[yes]/[no]:


Nov 11 2015 19:06:04: %PKI-CERTIFICATE_STATECHG-5: Certificate(issuer:C=CN, ST=BEIJING,
O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert, sn:4E95C7D7B1E3FC0B, subject:C=CN,
ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert) state valid

% PKI: Import Certificate success.
```

# Open the user certificate (topsec_rsa2_myself.pem), private key certificate (topsec_rsa2_myself.key) with Notepad, copy the content in these certificate respectively, enter command crypto ca import certificate to test on shell, follow the prompts to import the certificates to Device domain test in succession:

```
Device(config)#crypto ca import certificate to test

% Input the certificate data, press <Enter> twice to finish:

-----BEGIN CERTIFICATE-----

MIIDVTCCAr6gAwIBAgIQEJ7twbl3pDlzJz99DFOKOzANBgkqhkiG9w0BAQUFADBiMQswCQYDVQQGEwJ
DTjEQMA4GA1UECAwHQkVJSklORzEOMAwGA1UECgwFQ0lFQ0MxDzANBgNVBAsMBkdGQSBDQTEgM
B4GA1UEAwwXTWluaUNBIEZyZUJTRCBSb290IENlcnQwHhcNMTIwNjI2MDUwMTIzWhcNMzIwNjI2MDUw
MTIzWjB/MQswCQYDVQQGEwJDTjEQMA4GA1UECAwHYmVpamluZzESMBAGA1UEBwwJZG9uZ2NoZW
5nMQ4wDAYDVQQKDAVjaWVjYzEMMAoGA1UECwwDZ2ZhMR0wGwYJKoZIhvcNAQkBFg50ZXN0QGVjL
mNvbS5jbjENMAsGA1UEAwwEcnNhMjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA6AlNqTnNsV9
Yyij2tTMppB9C5VCLtkPh9KlIq/ZTlVhrJED+N5HVfQQyZYS/z4JWAip50dyP1+NP+bvP+pb9CfEaJ8+ObYQnf
UH6qiPccLkWO3XYanu6Dw5EMJYntwglSKmk1Pcc+j+yzWnwYMDFcbSsQ+8J5UzlesFhU7GnXacCAwEAA
aOB7jCB6zA+BgNVHR8ENzA1MDOgMaAvhi1odHRwczovLzIxMS44OC4yNS4xODo4NDQ0L2dmYS9jcmw
vUlNBMTAyNC5jcmwwUQYDVR0gBEowSDBGBggrBgEEAYcrMjA6MDgGCCsGAQUFBwIBFixodHRwczov
LzIxMS44OC4yNS4xODo4NDQ0L2dmYS9jcmwvUlNBMTAyNC5wbDALBgNVHQ8EBAMCA/gwCQYDVR0T
BAIwADAdBgNVHQ4EFgQUp/9/ODGLR84syxPaBkLG3mCpU5YwHwYDVR0jBBgwFoAUhnY8uZXbE2iX1m
XOipvfuDUgAeswDQYJKoZIhvcNAQEFBQADgYEAYrFZQrINHoLN9odcGctzTRGVmMcv9sJ0ncgUEfbrLu6
QUodQy3jjxWFIxheJK1btfF66/ShuKtZpqJ1WE9l92tfIHwLpXT0gujtxNi02TOPBNEU7P9nUgxgfDG+uhyPTeuf
Skfn3LCTHmGfVORF2soGSlaUPV1Zy5E9hmFZoMhs=

-----END CERTIFICATE-----


% Input the private key data, press <Enter> twice after data to finish or press <Enter> without data to ignore:

-----BEGIN RSA PRIVATE KEY-----

MIICXQIBAAKBgQDoCU2pOc2xX1jKKPa1MymkH0LlUIu2Q+H0qUir9lOVWGskQP43kdV9BDJlhL/PglYCKn
nR3I/X40/5u8/6lv0J8Ronz45thCd9QfqqI9xwuRY7ddhqe7oPDkQwlie3CCVIqaTU9xz6P7LNafBgwMVxtKxD7
wnlTOV6wWFTsaddpwIDAQABAoGBAMnJNWliJFgI4+1CvHGN4buhmApWBnnmBL1A7jrlh4CMGPi5MJrgz
vjeSnlwfWIXJXbSu4feuJT1UFqMkuyIm9l+k8Rm3hjClXIlfNV/ykG6a6GIVFYGxQWhaL50Pm6S7xXL9Ryd6hn
OHUUtwuLvkpBTx/4qvrIABDtXRjVglvApAkEA9BN1ZxM31BOyeB6KXvvmXD6/+dGaDfE4Dbcijy1LgKliaEBJ
00e/0R9ekg6myGTU2asJvPtkaXPqcwvU6+e2mwJBAPNfRTk9LzUlNmTV2DrsE9k3rbPnqqS9wb/mLUNdv2
FQeoY/Zf4qh0WXsug2q/6GPsvLUA7mbdArGFUwwQbw3+UCQQC8r25LSOgX40JM6g8+bq4fEcOHdSoLLT
eQIststC9yP3/75/cqhoUbPYz2jK0SriB+RWM53X46p4nPdo4b8P2RAkBGjoBLL+nXxooWgcjGjFrUxsedOLTI
PhtFvz2wIiWx2NsswISZQ0skae58VB1ZFSJvguoa58M+bsAHMrNDh+HhAkBcNAjKBDdVw0lI6bNoRGugEvu
o3Z3O0kbVcjzZld+4aVG4DzvEp1ZbsYRv9YPMtpnzmB7WZUshAL99nHnHxtbh

-----END RSA PRIVATE KEY-----


Nov 11 2015 19:06:56: %PKI-CERTIFICATE_STATECHG-5: Certificate(issuer:C=CN, ST=BEIJING,
O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert, sn:109EEDC1B977A43973273F7D0C538A3B,
subject:C=CN, ST=beijing, L=dongcheng, O=ciecc, OU=gfa, E=test@ec.com.cn, CN=rsa2) state valid

% PKI: Import Certificate success.
```

# Upon successful import of the certificates, use show crypto ca certificates to check whether they are in Valid status:

```
Device#show crypto ca certificates
Root CA Certificate:
  Status: Valid
  Serial Number: 4e95c7d7b1e3fc0b
  Subject: C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
  Issuer : C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
  Validity
    Start date: 2009-08-03 06:06:52
    End   date: 2019-08-03 06:06:52
  Key Type: RSA(1023 bit)
  Usage: General
  Fingerprint(sm3):18d39e4c50c9ad8b11446ac7ac1736f853ac92e769994b98233b48787562429c
  Fingerprint(sha1):ab3559e26384539ffcac3c76b5a5e7a1f7073dfb
  Associated Identity: test
       index: 3

My Certificate:
  Status: Valid
  Serial Number: 109eedc1b977a43973273f7d0c538a3b
  Subject: C=CN, ST=beijing, L=dongcheng, O=ciecc, OU=gfa, E=test@ec.com.cn, CN=rsa2
  Issuer : C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
  Validity
    Start date: 2012-06-26 05:01:23
    End   date: 2032-06-26 05:01:23
  Key Type: RSA(1024 bit)
  Usage: General
  Fingerprint(sm3):504599a2f170c51b62b2f8b0850f33a5595bc9e592d14eae9c90b1e59de35a89
  Fingerprint(sha1):080614a82cc4f3786458c585f9a58edf19da19bd
  Associated Identity: test
       index: 4
```

Step 4: The FTP Client uploads file(s) to and downloads file(s) from the FTP Server.

# FTP Client uploads file(s) to FTP Server:

```
Device#filesystem
Device1(config-fs)#copy file-system startup ftps 2.0.0.1 a a startup VerifyType peer


Copying!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Total 103440 bytes copying completed.
```

# FTP Client downloads file(s) from FTP Server:

```
Device(config-fs)#ftpscopy 2.0.0.1 a a test.doc test.doc VerifyType peer


Downloading####################################################################################
#################################################################################################
#################################################################################################
################################### OK!
```

Step 5: Check the result.

# Upon completion of the downloading, check the downloaded file(s) in the Device's file system:

```
Device(config-fs)#dir

   size         date         time      name

------------    ------       ------    --------

10189            NOV-04-2015  20:27:03   history

436578           NOV-04-2015  20:33:08   test.doc
```

5 File System Management

5.1 Overview

The following lists the storage medium of the device and their functions:

- SDRAM: Synchronous Dynamic Random Access Memory (SDRAM) provides the space for executing application programs of the device.
- FLASH: Stores application programs, configuration files, and the BootROM programs, and so on.
- EEPROM: Electrically Erasable and Programmable Read-Only Memory (EEPROM) stores system configuration files and user information which is frequently changed.

The device manages the following types of files:

- BootROM files: Store basic data for system initialization.
- Device application programs: Implement tasks such as route forwarding, file management, and system management.
- Configuration files: Store the system parameters that are configured by the users.
- Log files: Stores system log information.

The system has constructed one or more DOS-based file systems to store information which is rarely modified, including device application programs (protocol software and drivers) and BootROM. The file systems are called True Flash File Systems (TFFSs).

5.2 File System Management Function Configuration

Table 5-1 File System Management Function List

Configuration Tasks	
Manage storage devices.	Display the information about a storage device.
	Format a storage device.
Manage file directories.	Display the information about a file directory.
	Display the current working path.
	Change the current working path.
	Create a directory.

	Delete a directory.
Manage file operations	Copy a file.
	Rename a file.
	Display the content of a file.
	Delete a file.
Execute a configuration file manually.	Execute a configuration file manually.
Configure startup parameters.	Configure startup parameters.

5.2.1 Manage Storage Devices *-B -S -E -A*

Configuration Conditions

Before performing operations on storage devices, ensure that:

- The system has started normally.

Display the Information about a Storage Device

By displaying the information about a storage device, you can view the features of the storage device and the size of the remaining space.

Table 5-2 Displaying the Information about a Storage Device

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Display the information about a storage device.	**volume**	Mandatory

Format a Storage Device

If the space of a storage device is unavailable, you can use the format command to format the storage device.

Table 5-3 Formatting a Storage Device

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Format a storage device.	**format** { **/flash** | **/usb** }	Optional

NOTE

- Exercise caution in formatting a storage device, because the operation may cause permanent loss of all files on the storage device, and the files cannot be recovered.

Remove a Storage Device

When removing a storage device, first use the command to uninstall the file system and then remove the device securely.

Table 5-4 Remove a Storage Device

Step	Command	Description
Remove a storage device	**fschange** / *usb***remove**	Optional

NOTE

- Before removing the storage device, perform pop operations to the storage device in the windows operating system like. Otherwise, it may damage the file directory on the storage device which cannot be restored.
- This command can only be used to remove the USB.

5.2.2 Manage File Directories *-B -S -E -A*

Configuration Conditions

Before performing operations on file directories, ensure that:

- The system has started normally.

Display the Information about a File Directory

By displaying the information about a file directory, you can view the details of the files in the specified directory.

Table 5-5 Displaying the Information about a File Directory

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Display the information about a directory.	**dir** [*path*]	Mandatory

Display the Current Working Path

By displaying the current working path, you can view the details of the current path.

Table 5-6 Displaying the Current Working Path

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Display the current working path.	**pwd**	Mandatory

Change the Current Working Path

By changing the current working path, you can switch over a user to the specified directory.

Table 5-7 Changing the Current Working Path

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Change the current working path.	**cd** *path*	Mandatory

Create a Directory

If you want to create a directory in the file system, perform this operation.

Table 5-8 Creating a Directory

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Create a directory.	**mkdir** *directory*	Mandatory

Delete a Directory

If you delete a directory through this operation, all sub-directories and files in the directory are deleted.

Table 5-9 Deleting a Directory

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Delete a directory.	**rmdir** *directory*	Mandatory

NOTE

- Exercise caution when deleting a directory, because the operation of deleting the directory may permanently delete all sub-directories and files in the directory, and the files cannot be recovered.

5.2.3 Manage File Operations *-B -S -E -A*

Configuration Conditions

Before performing operations on files, ensure that:

- The system has started normally.

Copy a File

In the file system, you can copy a file to the specified directory.

Table 5-10 Copying a File

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-

Step	Command	Description
Copy a file.	**copy** *src-parameter dest-parameter*	Mandatory

NOTE

- The **copy** command can be used to copy file between the file system, the FTP server, and the TFTP server. For details, refers to the description of the **copy** command in the command manual.

Rename a File

In the file system, you can change the name of a file into a specified name.

Table 5-11 Renaming a File

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Rename a file.	**rename** *src-filename dest-filename*	Mandatory

Display the Content of a File

In the file system, you can view the content of a file.

Table 5-12 Displaying the Content of a File

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Display the content of a file.	**type** *path/filename*	Mandatory

Delete a File

In the file system, you can delete a file that is no longer in need.

Table 5-13 Deleting a File

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Delete a file.	**delete** *path/filename*	Mandatory

NOTE

- Exercise caution when you use the delete command because it permanently deletes a file, and the file cannot be recovered.

5.2.4 Download a File from FTP *-B -S -E -A*

Configuration Conditions

Before manually downloading the file from the FTP, first complete the following tasks:

- The system has started normally.
- Ensure that the route between the FTP server and the device interface is reachable and the route can be pinged through.

Download a File from the FTP Server

Use a command for downloading the file from the FTP and you can download the related file on the FTP server to the file system

Table 5-14 Download a File from the FTP Server

Step	Command	Description
Enter the file configuration mode	**filesystem**	-
Download the file from the FTP server	**ftpcopy** [**vrf** *vrf-name*] *host-ip-address usrname password src-filename* { **/flash** | /**usb** | *dest-filename* }	Optional

NOTE

- The **ftpcopy** command can be used to download the file from the FTP server to the file system. For details about the operation, refer to the using method of the **ftpcopy** command in the command manual.

5.2.5 Configure Startup Parameters *-B -S -E -A*

Configuration Conditions

Before configuring startup parameters, ensure that:

- The system has started normally.

Configure Startup Parameters

In configuring startup parameters, you can configure the application program file that is to be used in next startup.

Table 5-15 Configuring Startup Parameters

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Configure startup parameters.	**boot-loader** *path/filename* [*bootline-number*]	Mandatory

5.2.6 Monitoring and Maintaining of File System Management *-B -S -E -A*

Table 5-16 Monitoring and Maintaining of File System Management

Command	Description
clear boot-loader [*bootline-number*]	Clears the startup parameters with the specified index.
show filesystem	Display the information about the file system.
show file { **location | descriptor** }	Display the location of the system file in the file system and the descriptor.
show boot-loader	Display the system startup parameters.

5.3 Typical Configuration Example of File System Management

5.3.1 Configure Startup Parameters *-B -S -E -A*

Network Requirements

None

Network Topology

None

Configuration Steps

Step 1: Enter the file system configuration mode.

Step 2: Configure system startup options.

#View the system startup parameters.

```
Device#filesystem
Device(config-fs)#show boot-loader
The app to boot at the next time is: flash0: /flash/sp3-g-6.5.0.4.0.pck
The app to boot at the this time is: flash0: /flash/sp3-g-6.5.0.4.0.pck

Boot-loader0: flash0: /flash/sp3-g-6.5.0.4.0.pck

Device(config-fs)#exit
```

#Modify the file for next startup to the sp3-g-6.5.0.4.1.pck file that is stored in the flash, and set the priority to 0.

```
Device#filesystem
Device(config-fs)#boot-loader sp3-g-6.5.0.4.1.pck 0
Device(config-fs)#exit
```

#View the configuration result.

```
Device(config-fs)#show boot-loader
The app to boot at the next time is: flash0: /flash/sp3-g-6.5.0.4.1.pck
The app to boot at the this time is: flash0: /flash/sp3-g-6.5.0.4.0.pck
```

6 Configuration File Management

6.1 Overview

Configuration file management is a function that is used to manage device configuration files. Through the command line interface provided by the device, users can easily manage configuration files. If the device needs to automatically load the current configuration of users after restart, the current configuration commands must be saved into the configuration file before the device restarts. Users can upload configuration files to or download configuration files from another device through FTP or TFTP, realizing batch device configuration. The device configuration is categorized into the following two types:

Startup configuration:

When the device starts, it loads the startup configuration file with the name "startup" by default, and it completes the initialization configuration of the device. This configuration is called startup configuration. Here the device has two startup configuration files, one is the default startup configuration file, and the other is the backup startup configuration file. When the device starts, if the default startup configuration file does not exists, the system copies the backup startup configuration file to the location of the default startup configuration file and loads this startup configuration file.

Current configuration:

Current configuration is a set of commands that take effect currently. It consists of startup configuration and the configuration that is added or modified by the user after startup. The current configuration is saved in the memory database. If the current configuration is not saved into the startup configuration file, the configuration information gets lost after the device restarts.

The following describes the contents and formats of the configuration files:

- Configuration files are saved in the file system in the form of text files.
- The contents of the configuration files are saved in the form of configuration commands, and only non-default configuration is saved.
- Configuration files are organized based on command modes. All commands in one command mode are organized together to form a paragraph.
- Paragraphs are organized according to a certain rule: system configuration mode, interface configuration mode, and configuration modes of different protocols.
- Commands are organized according to their relations. The related commands form a group, and different groups are separated by blank lines.

6.2 Configuration File Management Function Configuration

Table 6-1 Configuration File Management List

Configuration Tasks	
Save the current configuration.	Save the current configuration.
Back up device configuration.	Back up the current configuration.
	Back up the startup configuration.
Restore the startup configuration.	Restore the startup configuration.

6.2.1 Save the Current Configuration *-B -S -E -A*

Configuration Conditions

None

Save the Current Configuration

If the current configuration of the user can take effect only after the device starts, you need to save the current configuration into the startup configuration file.

Table 6-2 Saving the Current Configuration

Step	Command	Description
Save the current configuration to the startup configuration file.	**write**	Mandatory

NOTE

- If the device is restarted or powered off while the configuration file is being saved, configuration information may get lost.
- Saving the current configuration not only saves the configuration to the startup configuration file, but also saves the configuration to the backup startup configuration file.

6.2.2 Configure the Backup System *-B -S -E -A*

Configuration Conditions

Before configuring the backup system parameters, ensure that:

- The route between the device and the server is reachable.

- The configuration file to be backed up exists; otherwise, backup fails.

Back Up the Current Configuration

In backing up the current configuration, you can use a command to back up the current configuration to the FTP server.

Table 6-3 Backing Up the Current Configuration

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Back up the current configuration to a remote host through the FTP protocol.	**copy running-config** { **file-system** *dest-filename* | **ftp** [**vrf** *vrf-name*] { *hostname* | *ip-address* } *username password dest-filename* | **startup-config** | **tftp** [**vrf** *vrf-name*] { *hostname* | *ip-address* } *dest-filename* }	Mandatory

Back Up Startup Configuration

In backing up the startup configuration, you can use a command to back up the startup configuration to the FTP server.

Table 6-4 Backing Up the Startup Configuration

Step	Command	Description
Enter the file system configuration mode.	**enable**	-
Save the startup configuration to a remote host through the FTP protocol.	**copy startup-config** { **file-system** *dest-filename* | **ftp** [**vrf** *vrf-name*] { *hostname* | *ip-address* } *username password dest-filename* | **tftp** [**vrf** *vrf-name*] { *hostname* | *ip-address* } *dest-filename* }	Mandatory

6.2.3 Restore the Startup Configuration *-B -S -E -A*

Configuration Conditions

Before restoring the startup configuration, ensure that:

- The route between the device and the server is reachable.
- The configuration file that is to be restored exists.

Restore the Startup Configuration

In restoring the startup configuration, you can use a command to download the startup configuration file from the FTP server and set it as the startup configuration file that is used after restart. In this way, after the device is restarted, the device can load the startup configuration file.

Table 6-5 Restoring the Startup Configuration

Step	Command	Description
Enter the file system configuration mode.	**filesystem**	-
Restore the startup configuration.	**copy** { **file-system** *src-filename* **| ftp** [**vrf** *vrf-name*] { *hostname* | *ip-address* } *username password src-filename* | **tftp** [**vrf** *vrf-name*] { *hostname* | *ip-address* } *src-filename* } { **file-system** *dest-filename* **| startup-config** }	Mandatory

NOTE

- Before overwriting the local startup configuration, ensure that the configuration file matches the device type and matches the current system version.
- After performing the operation of restoring the startup configuration, the current configuration is not changed. After the device is restarted, the startup configuration is restored.

6.2.4 Monitoring and Maintaining of Configuration File Management *-B -S -E -A*

Table 6-6 Monitoring and Maintaining of Configuration File Management

Command	Description
show running-config [**after-interface** | **before-interface | interface** [*interface-name*] | [*configuration*]] [| { { **begin | exclude | include** } *expression* | **redirect** { **file** *file-name* **| ftp** [**vrf** *vrf-*	Display the current configuration information.

Command	Description
name] { *hostname* | *ip-address* } *user-name password file-name* } }]	
show startup-config [*file-number* | { **|** { { **begin** | **exclude** | **include** [**context**] } *expression* | **redirect** { **file** *filename* **|** **ftp** { [**vrf** *vrf-name*] { *hostname* **|** *ip-address* } *user-name password file-name* } } }]	Display the startup configuration information.

6.2.5 Configuration File Encryption -B -S -E -A

Configuration Conditions

- A USB Device has to be plugged in in order to encrypt the configuration file.

Configure for Configuration File Encryption

Configuration file encryption refers to the encryption of configuration file using Chinese encryption algorithm SM4 with user designated cryptographic key. After the user has designated a cryptographic key, the configuration file will be encrypted during the next performance of write.

Operation record encryption refers to the encryption of configuration file using Chinese encryption algorithm SM4 with user designated cryptographic key. After the user has designated a cryptographic key, later operation records will be encrypted.

Table 6–7 Configuration File Encryption & Operation Record Encryption

Steps	Command	Description
Enter global configuration mode	**config terminal**	-
Configuration file encryption	**service encryption startup algorithms SM4 key** *password*	Configuration file encryption, user designated cryptographic key
Operation record encryption	**service encryption history algorithms SM4 key** *password*	Operation record encryption, user designated cryptographic key

NOTE

- The encryption of configuration file will take effect at the next performance of write action after the encryption function is configured. The encryption of operation records takes effect immediately after the encryption function is configured.
- To configure the encryption function, an external USB Device has to be plugged in. Operation record encryption function does not require the USB Device.

7 System Management

7.1 Overview

- Through system management, users can query the current working status of the system, configure basic function parameters of the device, and perform basic maintenance and management operations on the device. The system management functions include: Configuring the device name
- Configuring the system time and time zone
- Configuring the login welcome message
- Configuring the system exception processing mode
- Restarting the device
- Configuring the password encryption service
- Configuring the history command saving function
- Configuring the login security service
- Configuring CPU monitoring
- Configuring display of properties in pages

7.2 System Management Function Configuration

Table 7-1 System Management Function List

Configuration Tasks	
Configure the device name.	Configure the device name.
Configure the system time and time zone.	Configure the system time and time zone.
Configure the login welcome message.	Configure the login welcome message.
Configure the system exception processing mode.	Configure the system exception processing mode.
Configure to restart the device.	Configure to restart the device.

Configuration Tasks	
Configure the encryption service.	Configure the encryption service.
Configure the history command saving function.	Configure the history command saving function.
Configure the login security service.	Configure the login security service.
Configure CPU monitoring.	Configure CPU monitoring.
Configure display of properties in pages.	Configure display of properties in pages.

7.2.1 Configure the Device Name *-B -S -E -A*

Configuration Conditions

None

Configure the Device Name

A device name is used to identify a device. A user can change the device name according to the actual requirement. The modification takes effect immediately, that is, the new device name is displayed in the next system prompt.

Table 7-2 Configuring the Device Name

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the device name.	**hostname** *host-name*	Mandatory

7.2.2 Configure the System Time and Time Zone *-B -S -E -A*

Configuration Conditions

None

Configure the System Time and Time Zone

The system time and time zone is the time displayed in the timestamp of system information. The time is determined by the configured time and time zone. You can run the **show clock** command to view the time information of the system. To make the device work normally with other devices, the system time and time zone must be accurate.

Table 7-3 Configuring the System Time and Time Zone

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the system time.	**clock timezone** *timezone-name-string hour-offset-number* [*minute -offset-number*]	Mandatory. The default is Universal Time Coordinated (UTC).
Enter the privileged user mode.	**exit**	-
Configure the system time.	**clock** *year-number* [*month-number* [*day-number* [*hour-number* [*minute-number* [*second-number*]]]]]	Mandatory

7.2.3 Configure the Login Welcome Message *-B -S -E -A*

Configuration Conditions

None

Configure the Login Welcome Message

When a user logs in to the device for login authentication, the login welcome message is displayed. The welcome message can be configured according to the requirement.

Table 7-4 Configuring the Login Welcome Message

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the login welcome message.	**banner motd** *banner-line*	Mandatory

7.2.4 Configure the System Exception Processing Mode *-B -S -E -A*

Configuration Conditions

None

Configure the System Exception Processing Mode

When a system exception occurs, the system directly restarts to restore the system. The system exception processing mode is configured in two aspects: The first is enabling periodical exception detection. The system periodically detects the task status, code segment, and semaphore dead lock with a cycle of 10s, 10s, and 30s respectively. Secondly, an exception level is configured. If exceptions of the level and higher levels occur, the device restarts. Exception levels include: alert, critical, emergency, error, and warn.

Table 7-5 Configuring the System Exception Processing Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the system exception processing mode	**exception** { **period-detect enable** | **reboot** [**level** { **alert** | **critical** | **emergency** | **error** | **warn** }] }	Mandatory. By default, periodical exception detection is enabled, and the exception level set for device restart is critical.

NOTE

- After an exception level is configured for device restart, if an exception at the level or a higher level occurs, the device restarts.
- From high to low, exception levels include emergency, alert, critical, error, and warn.

7.2.5 Configure to Restart a Device *-B -S -E -A*

Configuration Conditions

None

Restart a Device

When a device fault occurs, you can choose to restart the device according to the actual situation so as to eliminate the fault. The device restart modes include cold restart and hot restart. In a cold restart, the user can directly power off the device and power on the device again. In a hot restart, the user restarts the device by using a restart command. During the hot restart process, the device is not powered off.

Table 7-6 Restarting a Device

Step	Command	Description
Use a command to restart the device.	**reload**	Mandatory

NOTE

- If you forcedly power off and restart a device that is in the operating status, hardware damage or data loss may be caused. Therefore, this restart mode is usually not recommended.
- If you use the reload command to restart the device, all the services of the device are interrupted. Exercise caution when performing this operation.

7.2.6 Configure the History Command Saving Function *-B -S -E -A*

Configuration Conditions

None

Configure the History Command Saving Function

Through the history command saving function, you can query and collect the history commands that have been executed. Before the history command saving function is configured, history commands are saved in the memory file system. After the function is configured, the system automatically saves history commands in the flash file system.

Table 7-7 Configuring the History Command Saving Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure to save history commands.	**service shell-history**	Mandatory. By default, the history command saving function is disabled.

7.2.7 Configure the Login Security Service *-B -S -E -A*

Configuration Conditions

None

Enable the System Login Security Service

To enhance the system security, the device provides the system login security service function. The functions include:

- Prevents brute force cracking of user login passwords.
- Prevents the fast connection function.

The function of brute force cracking prevention prevents malicious illegal users from forcedly cracking the user name and password for logging in to the device. If the system finds that the number of continuous login authentication failures of a user reaches the number specified by the system, the system rejects the login request from the IP address within the specified period of time.

The function of preventing fast connections prevents illegal users from initiating a large number of login requests within a short period time because this may occupy a lot of system and network resources. If the number of repeated login connections from a user reached a specified number, the system rejects the login connection requests from the IP address within the specified period of time.

Table 7-8 Enabling the System Login Security Service

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the system login security service.	**service login-secure**	Mandatory. By default, the system login security service is disabled.

Configure the Parameters of the System Login Security Service

Table 7-9 Configuring the Parameters of the System Login Security Service

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the interval at which login security service records are checked to see whether they are aged.	**login-secure check-record-interval** *check-record-interval-number*	Mandatory. The default is 60 minutes.
Configure a period of time in which login requests from a specified IP address are rejected.	**login-secure forbid-time** *forbid-time-number*	Mandatory. The default is 10 minutes.
Configure the maximum allowed number of	**login-secure max-try-time** *max-try-time-number*	Mandatory. The default number is 5.

Step	Command	Description
continuous login authentication failures.		
Configure the aging time of records.	**login-secure record-aging-time** *record-aging-time-number*	Mandatory. The default is 15 minutes.
Configure the maximum number of fast connections.	**login-secure quick-connect max-times** *max-times-number*	Mandatory. The default number is 20.
Configure the minimum interval of fast connections.	**login-secure quick-connect restrict-interval** *restrict-interval-number*	Mandatory. The default number is 30s.
Configure the time during which login connections are rejected.	**login-secure quick-connect unrestrict-interval** *unrestrict-interval-number*	Mandatory. The default is 20 minutes.

7.2.8 Configure CPU Monitoring *-B -S -E -A*

Configuration Conditions

None

Configure CPU Monitoring

Through CPU monitoring, the system monitors the CPU occupancy to learn the current operation status of the CPU. The following shows the contents of CPU monitoring:

- Monitors the CPU occupancy of each process. After the function is configured, you can view the related information by using the **show cpu** command.
- Enables the history statistics function of the CPU occupancy. After the function is configured, you can view the related information by using the **show cpu monitor** command.

Table 7-10 Configuring CPU Monitoring

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable CPU occupancy monitoring of the processes.	**spy cpu**	Mandatory.

Step	Command	Description
		By default, CPU occupancy monitoring is disabled.
Enable history statistics of CPU occupancy.	**monitor cpu**	Mandatory. By default, history statistics of CPU occupancy is enabled.
Configure the network management monitoring of CPU information.	**check cpu** { **enable** | **disable** | **parameter** | { **time-interval** *time-interval-value* } | { **view** [**simple**] } }	Mandatory. By default, network management monitoring of CPU occupancy is not configured.

7.2.9 Configure Display of Properties in Pages *-B -S -E -A*

Configuration Conditions

None

Configure Display of Properties in Pages

System information can be displayed in pages, making it easy for users to view the information. Users can set to display device information in pages according to the actual requirement.

Table 7-11 Configuring Display of Properties in Pages

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure display of properties in pages.	**more** { **on** | **off** | **displine** [*num*] }	Mandatory. By default, the function of display in pages is enabled. By default, 24 lines are displayed in **displine**.

7.2.10 Operation Record File Management *-B -S -E -A*

Configuration Conditions

None

Configure Operation Record File

By default, operation records are saved in flash. Operation record file management mainly involves the change of the storage location of the operation records.

Table 7- 13 Configuration File Encryption & Operation Record Encryption

Steps	Command	Description
Enter global configuration mode	**config terminal**	-
Operation record file management	**shell-history location** *device-name*	User designated storage location of operation records
Designation of operation record file size	**shell-history file max-size** *num*	User designated file size of operation records

7.2.11 System Management Monitoring and Maintaining *-B -S -E -A*

Table 7-12 System Management Monitoring and Maintaining

Command	**Description**
show clock	Display the information about the system clock.
show cpu	Display the information about the CPU usage.
show cpu check	Display the CPU occupancy of the processes that are monitored by the network management system.
show device	Display the device information of the system.
show environment	Display the information about the board temperature.
show history | { { **begin** | **exclude** | **include** } *expression* | **redirect** { **file** *file-name* | **ftp** [**vrf** *vrf-name*] { *hostname* | *ip-address* } *user-name password file-name* } }	Display the information about history commands.

Command	Description
show language	Display the information about system language version.
show login-secure information	Display the information about the system login security service.
show login-secure quick-connect	Display the fast connection information about system login security.
show mbuf allocated [*pool-name*]	Display the mbuf information.
show memory [**detail** | **fpss** | **free** | **heap** | **mbuf** | **slab** | **utilization**]	Display the memory information.
show netbuffer [**stat**]	Display the netbuffer memory information.
show pool [**detail** | **information**]	Display the information about the memory pool.
show process [*task-name*]	Display the main tasks in the system and their operating statuses.
show semaphore { *sem-name* | **all** | **binary** | **counting** | **list** | **mutex** } [**any** | **pended** | **unpended**]	Display the information about the system semaphore.
show spy	Display the status of the monitoring switch.
show stack	Display the usage of each task stack in the system.
show system fan	Display the fan information.
show system lpu	Display the LPU information.
show system module brief	Display brief information about all module part of the device.
show system mpu	Display the MPU information.
show system power	Display the power supply information.

Command	Description
show tech-support { sys-base [detail] | l2-base [detail] | l3-base [detail] | all } [**page** | **to-memory** | **to-flash**]	Display the technical support information.
show version [**detail**]	Display the system version information.

7.3 Example of System Management Typical Configuration

7.3.1 Configure User-based or IP-based Login Limitation *-B -S -E -A*

Network Requirements

- PC1, PC2 are used as local terminals, which can log on to the Device via Telnet, ssh.
- Device can limit certain user and IP's login to PC1, PC2.

Network Topology

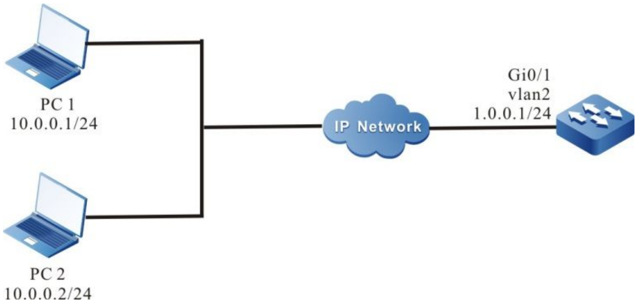


Figure 7-1 Networking Diagram - Configure User- or IP-based Login Limitation

Configuration Steps

Step 1: Configure the interfaces' IP addresses, and configure routing protocol for connectivity between PC1/PC2 and Device. (omitted)

Step 2: Configure user- or IP-based login limitation function.

# Enable login security function of telnet, ssh.

```
Device#configure terminal
Device(config)#service login-secure telnet
Device(config)#service login-secure ssh
```

# Configure the maximum number of telnet and ssh login attempts to 5 for an IP address and 5 for all users.

```
Device(config)#login-secure telnet ip-addr max-try-time 5
Device(config)#login-secure telnet user max-try-time 5
Device(config)#login-secure ssh ip-addr max-try-time 5
Device(config)#login-secure ssh user max-try-time 5
```

Step 3: Enable the Device's ssh service, configure user name and password, and set up for login by local authentication

```
Device(config)#ip ssh server
Device(config)#user user1 password 0 admin
Device(config)#line vty 0 15
Device(config-line)#login local
Device(config-line)#exit
```

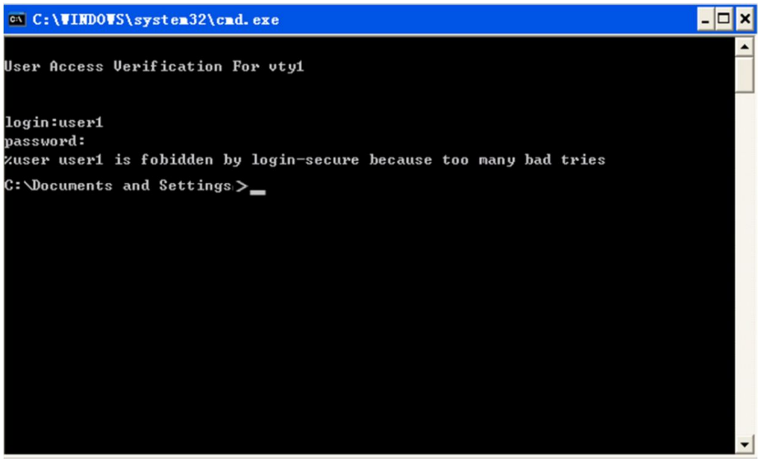
Step 4: Check the result.

# Use PC1 try to log on to the Device via telnet with user name user1; after 6 consecutive login attempts with incorrect password, check the Device's telnet login security statistics for user information:

```
Device#show login-secure telnet user
telnet module forbidden user information:
user         try-time  forbid-time      wd-id          number      record-time
---------     --------  -----------      ------          ------      -----------
user1         6        00:09:00         0x167f9c20      0          00:01:00
```

It is expected that user1 is deemed as a login attacker and that user1 is denied access to log on to the Device via telnet for 10 minutes.

Try to use PC1 to log on to the Device via telnet with user name user1, a message prompting access denied is expected.



```
User Access Verification For vty1

login:user1
password:
%user user1 is fobidden by login-secure because too many bad tries
C:\Documents and Settings>_
```

# Use PC2 try to log on to the Device via ssh, using a user name not configured in the Device; after 6 consecutive login attempts, check the Device's ssh login security statistics for IP information:

```
Device#show login-secure ssh ip-addr
ssh module forbidden login address:
client address  try-time  forbid-time     wd-id      type     number  record-time
```

```
--------------  --------  -----------     ------     ------    ------  -----------
10.0.0.2       6        00:09:00        0x167f9c80  login     0       00:01:00
```

It is expected that PC2's IP address is deemed as an attacking IP address and that PC2 is denied access to log on to the Device via ssh for 10 minutes.

Try to use PC2 to log on to the Device via ssh, a message prompting access denied is expected.

NOTE

- Only when the configured maximum number of allowable attempts is exceeded will the further attempts be considered as login attacks and denied access.
- Some PC ssh clients at times of login failure would initiate internal retry and such retries would be recorded by the Device as multiple login attempts.
- By default, telnet/ssh login security function is enabled on the Device.

7.3.2 Configure Fast Login Limitation *-B -S -E -A*

Network Requirements

- PC1, PC2 are used as local terminals, which can log on to the Device via Telnet.
- PC1 will be denied access to login the Device after repetitive fast login attempts, in such cases, PC2 is not affected.

Network Topology

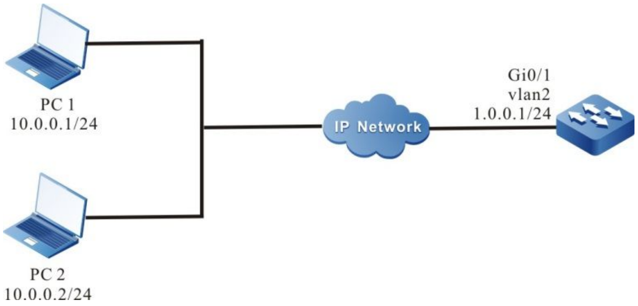


Figure 7-2 Networking Diagram - Configure Fast Login Limitation

Configuration Steps

Step 1: Configure the interfaces' IP addresses, and configure routing protocol for connectivity between PC1/PC2 and Device. (omitted)

Step 2: Configure fast login limitation function for telnet.

# Enable telnet login security function, and configure the maximum number of fast login attempts to 20 and duration of denial period to 10.

```
Device#configure terminal
```

```
Device(config)#service login-secure telnet
Device(config)#login-secure telnet quick-connect max-times 20
Device(config)#login-secure telnet quick-connect forbid-time 10
```

Step 3: Configure the user name and password for login the Device, and configure to use local authentication login.

```
Device(config)#user user1 password 0 admin
Device(config)#line vty 0 15
Device(config-line)#login local
Device(config-line)#exit
```

Step 4: Check the result.

# Use PC1 to login/logout repetitively 21 times at an interval no more than 30 seconds via telnet with user name user1, then check the Device's telnet login security statistics for fast connection information:

```
Device#show login-secure telnet quick-connect
telnet module quick connect info:
connect ip      connect times  last connect time          forbid-time     record-time
----------      -------------  -----------------          -----------     -----------
10.0.0.1        21           TUE AUG 11 20:22:38 2015    00:09:00        00:01:00
```

It is expected that PC1 is considered as a login attacker address and that PC1 is denied access to log on to the Device via telnet for 10 minutes.

In such cases, use PC2 can successfully log on to the Device via telnet.

8 System Alarm

8.1 Overview

With the system alarm function, if an exception occurs, the system sends an alarm prompt message so that the user can pay attention to the exception of the device and take the corresponding measures to ensure stable operation of the device. System alarms include temperature alarms, power supply abnormality alarms, and fan abnormality alarms. For the system temperature alarms, if the CPU or environment temperature reaches the threshold, abnormal system alarm log information is generated. By default, the CPU temperature alarm threshold is 100° and the environment temperature alarm threshold is 80°. Power supply and fan exceptions also generate abnormal system alarm log information.

8.2 System Alarm Function Configuration

Table 8-1 System Alarm Function List

Configuration Tasks	
Configure system temperature alarms.	Configure system temperature alarms.
Configure system power supply alarms.	Configure system power supply alarms.
Configure system fan alarms.	Configure system fan alarms.

8.2.1 Configure System Temperature Alarms *-B -S -E -A*

Configuration Conditions

Before configuring system alarms, ensure that:

- After the system is started and operates stably, all boards are loaded successfully.
- After the system is started and operates stably, the power supply and fans operate normally.

Configure System Temperature Alarms

In configuring system temperature alarms, you need to configure the temperature threshold for CPU or environment alarms. If the CPU temperature or environment temperature reaches the threshold, system alarm log information is generated. By default, the CPU temperature alarm threshold is 100° and the environment temperature alarm threshold is 80°.

Table 8-2 Configuring System Temperature Alarms

Step	**Command**	**Description**
Enter the global configuration mode.	**config terminal**	-
Configure the threshold for CPU or environment temperature alarms.	**alarm temperature mpu** { **cpu** | **environment** } *temperature*	Mandatory.

8.2.2 Configure System CPU Alarms *-B -S -E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of system alarms:

- All on-board cards have been successfully loaded after the system is started and stabilized.

Configure System CPU Alarms

Configuration of system CPU alarms refers to the configuration of a CPU utilization monitoring threshold. When CPU utilization rate exceeds the threshold, an alarm of abnormal CPU utilization will be triggered.

Table 8–3 Configure System CPU Alarms

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure system CPU utilization alarm threshold	**cpu utilization warner-threashold** [*rate-value*]	Optional

8.2.3 Configure A Low Threshold Value for System Memory Use *-B -S -E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of system threshold alarms:

- All on-board cards have been successfully loaded after the system is started and stabilized.

Configure A low Threshold Value for System Memory Use

The low threshold value for system memory utilization refers to a value which, when configured for and exceeded by system memory utilization, indicates that the system is short of available memory.

Table 8–4 Configure System Memory Threshold Alarms

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure system memory threshold alarms	**memory threshold low** *low-value*	Optional By default, the system memory low threshold value is 32M.

8.2.4 Configure System Memory Alarms **-B -S -E -A**

Configuration Conditions

The following tasks have to be completed prior to the configuration of system alarms:

- All on-board cards have been successfully loaded after the system is started and stabilized.

Configure System Memory Alarms

Configuration of system memory alarms refers to the configuration of a monitoring threshold for system memory utilization. When this monitoring threshold is exceeded, an alarm of abnormal system memory utilization will be triggered.

Table 8–5 Configure System Memory Alarms

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure system memory utilization alarm threshold	**memory utilization warner-threashold** [*rate-value*]	Optional By default, the system memory utilization alarm threshold value is 95%.

8.2.5 Configure System Power Supply Alarms ***-B -S -E -A***

Configuration Conditions

None

Configure System Power Supply Alarms

If a power supply fault or exception occurs, the system immediately generates log information about system power supply alarms. This helps the user to pay attention to the exception of the device power supply and take the corresponding measures to get rid of the fault and ensure stable operation of the device. By default, the system power supply alarm function is enabled.

8.2.6 Configure System Fan Alarms *-B -S -E -A*

Configuration Conditions

None

Configure System Fan Alarms

If a system fan fault or exception occurs, the system immediately generates log information about the system fan alarm. This helps the user to pay attention to the exception of the device fans and take the corresponding measures to get rid of the fault and ensure stable operation of the device. By default, the system fan alarm function is enabled.

9 System Log Configuration

9.1 Overview

System log information is categorized into eight levels, including: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**. Here levels 0-6 are log information and level 2 is debugging information. For details, refer to the following table.

Table 9-1 Description of the System Log Level Fields

Field	Level	Description
emergencies	0	Fatal fault. The system is unavailable, the device stops and it needs to be restarted.
alerts	1	Serious error. Functions of a certain type become unavailable, and the services are stopped.
critical	2	Critical error. Irreversible problems occur on the functions of a certain type, and some functions are affected.
errors	3	Error message.
warnings	4	Warning message.
notifications	5	Event notification message.
informational	6	Message prompt and notification.
debugging	7	Debugging message.

System log information is outputted to four directions: control console (Console terminal), monitor console (Telnet or SSH terminal), log server, and log files (memory log files and flash log files). The output to the four directly is controlled by respective configuration commands. The debugging information is outputted to two directions, control console and monitor console. In some special cases, the debugging information can also be configured to output to the log server or log files.

Table 9-2 Log Output Directions

Log Output Direction	Description
Control console	System log information is outputted to the Console terminal.
bootloader console	System log information is outputted to the Telnet or SSH terminal.
Log server	System log information is outputted to the log server. By default, logs of levels 0-5 are outputted to the log server.
Log files	System log information is outputted to the system memory or flash memory. By default, log information of levels 0-5 is outputted to the system memory, and log information of levels 0-4 is outputted to the flash memory.

The outputted system logs are first saved in the buffer of the log module. The buffer is shared by all information, therefore, if a large amount of information is outputted, logs may get lost. At this time, the log module collects statistics of the lost information and output the information. The log module then obtains the logs one by one from the buffer at the background, and outputs the logs at different output directions according to the log types. If congestion (such as Console die-hard or Telnet terminal exception) occurs at an output direction during the output process, after the daemon task of the log module detects the congestion, it restarts a new background output task to take over the existing task. In the new task, the direction with the congestion is closed, and the previous task automatically exits after the congestion is automatically removed. The following figure shows the schematic diagram.

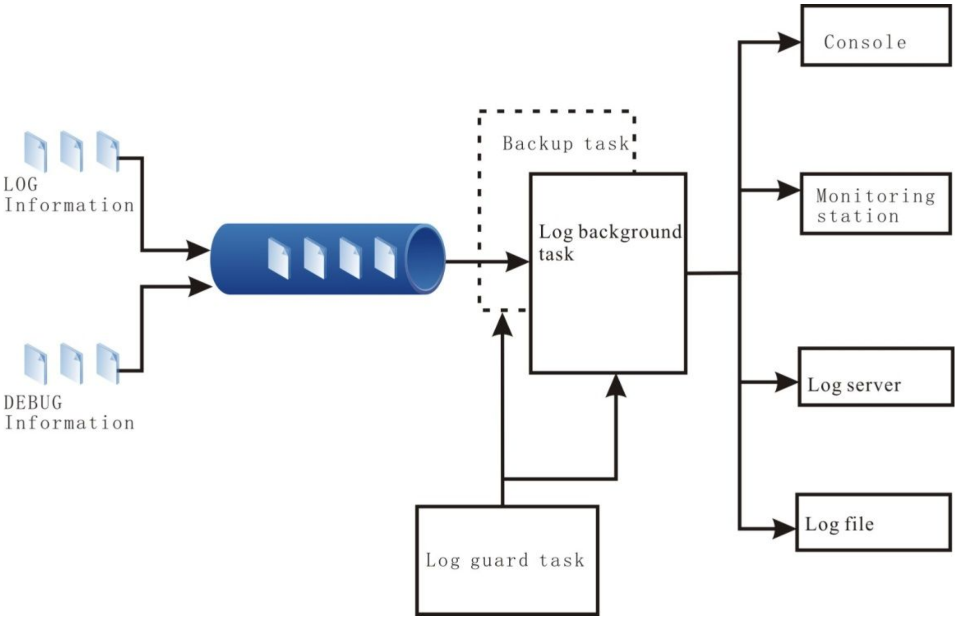


Figure 9-1 System Log Schematic Diagram

9.2 System Log Function Configuration

Table 9-3 System Log Function List

Configuration Tasks	
Configure log output functions	Configure log output to the control console.
	Configure log output to the monitor console.
	Configure log output to the server.
	Configure log output to files.
Configure the timestamp for logs.	Configure the timestamp for logs.
Configure a log task name.	Configure a log task name.
Configure the log filtration function.	Configure the log filtration function.
Configure the log server function.	Configure the log server function.
Configure the log file capacity.	Configure the log file capacity.
Configure log display colors.	Configure log display colors.

9.2.1 Configure Log Output Functions *-B -S -E -A*

Configuration Conditions

None

Configure Log Output to the Control Console

The control console refers to a Console terminal. It is a channel through which the system output log information to the control console. To view output of log information on the control console, you need to enable the log display function of the console.

Table 9-4 Configuring Log Output to the Control Console

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Enable log display on the control console.	**logging console** [*logging-level*]	Optional. By default, log display on the control console is enabled.

Configure Log Output to the bootloader Console

The monitor console refers to the Telnet or SSH terminal. It is used for remote device management. To configure displaying of log output to the monitor console, you need to enable the log display function of the global monitor console and enable log display on the current terminal. To speed up log display, you can disable the log display function of the console.

Table 9-5 Configuring Log Output to the bootloader Console

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Enable log display on the monitor console.	**logging monitor** [*logging-level*]	Optional. By default, the log display function of the global monitor console is enabled.
Enable log display of the current monitor console.	**terminal monitor**	Mandatory. By default, log display on the current monitor console is disabled.

Configure Log Output to the Server

To keep system log information in a more comprehensive manner, you can set up a log server for the devices in the same workgroup. Then the server receives the log information sent by the device. This facilitates system maintenance and management. In some special cases, the local device can also acts as the log server to receive log information from other device. For details, refer to the sections in log server configuration.

Table 9-6 Configuring Log Output to the Log Server

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Enable log output to the log server.	**logging trap**	Optional. By default, the log output to the log server function is enabled.
Configure log output to the log server.	**logging** *logging-server* [**vrf** *vrf-name*] [*logging-level* | **port** *port-num* [*logging-level*]]	Mandatory. By default, lot output to the log server is disabled.
Configuring the source address for sending log information.	**logging source-ip** *ip-address*	Optional. By default, the outgoing interface for sending log information is determined according to the route. The main IP address of the outgoing interface acts as the source IP address for sending log information.
Configure the log transmission type.	**logging facility** *logging-type*	Optional. By default, the log transmission type is local7(23).

Configure Log Output to Files

Log files can be stored in two manners, in the memory, and in the flash memory. The memory stores only log information from device startup to restart. By default, log information of level 5 (notifications) and higher levels are stored. By default, the flash memory stores log information of level 4 (warnings) and higher levels. For the levels of logs, refer to the detailed description in the following table. Both the two types of log files have capacity limit. When the size of log files reaches the maximum allowed capacity, the oldest log record is overwritten by the latest one.

Table 9-7 Configuring Log Output to Files

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the log output function.	**logging enable**	Optional. By default, the log output function is enabled.
Configure logs to be saved into the flash memory.	**logging file** [*logging-level*]	Optional. By default, the function of saving logs into the flash memory is enabled.
Configure logs to be saved into the memory.	**logging buffer** [*logging-level*]	Optional. By default, the function of saving logs into the memory is enabled.

9.2.2 Configure the Timestamp for Logs *-B -S -E -A*

Configuration Conditions

None

Configure the Timestamp for Logs

The timestamp of a log records in details the time at which the log is generated. By default, log timestamps adopt the Datetime (absolute time) format, but they also support Uptime (relative time) format. The absolute time format records the year and the time with millisecond precision. It outputs the time of logs in details, therefore, the absolute time format is recommended.

Table 9–8 Configure the Timestamp for Logs

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the timestamp for logs.	**service timestamps** { **log** | **debug** } [**uptime** | **datetime** [**localtime** / **msec** / **show-timezone / year**]]	Optional. By default, log timestamps adopt the absolute time format, but display of year and millisecond precision is disabled.

NOTE

- The uptime refers to the run time starting with device startup.
- The datetime refers to the time of the real-time clock.
- The localtime refers to local time.

9.2.3 Configure the Log Server Function *-B -S -E -A*

Configuration Conditions

None

Configure the Log Server Function

To facilitate centralized management of log information, you need to configure a log server to receive log information from the devices in the same working group. If a log server is not available temporarily, you can configure the local device as the log server to manage log information in a centralized manner. In configuring the function, you need to specify the open port and server log file capacity.

Table 9-9 Configure the Log Server Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the log server function.	**logging server** [**display** | **not-save** | **file-max-size** *file-size* | **port** *port-num*]	Optional. By default, the log server function is disabled.

NOTE

- If you run the **logging server display** or **logging server not-save command**, the log server function is automatically enabled.

9.2.4 Configure Logging Duplicates Suppression -B -S -E -A

Configuration Conditions

None

Configure Logging Duplicates Suppression

Under certain circumstances, the module may keep exporting identical logs incessantly, affecting the observation of other logs. At such moments, logging duplicates suppression function can be enabled. Duplicate log information will be exported only once in a suppression cycle, and the number of suppressions of the log in a cycle will be exported at the end of the suppression cycle.

Table 9–10 Configure Logging Duplicates Suppression

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure logging duplicates suppression function	**logging suppress duplicates interval** *interval-num*	Required By default, logging suppression function is enabled

9.2.5 Configure Log File Capacity -B -S -E -A

Configuration Conditions

None

Configure Log File Capacity

Due to the capacity limit of flash memory, the configurable range of the capacity of log file is 1M~32M. When the stored log information exceeds the configured maximum capacity limit, new logs will overwrite old ones (new files will overwrite old ones).

Table 9–11 Configure Log File Capacity

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure log file capacity	**logging file size** *file-max-size*	Optional By default, log file capacity is 1M bytes

9.2.6 Configure Log File Encryption *-B -S -E -A*

Configuration Conditions

None

Configure Log File Capacity

In view of the security of log information, the log files stored in flash can be encrypted. After the log file encryption function is configured, the subsequent logs will be stored in the log file in the form of cipher text. If the password of the log file changes, the logs previously stored in cipher text will not be displayed in plain text. Only if the password is re-configured as the one when the log is generated, the log information can be displayed in plain text.

Table 9–12 Configure Log File Encryption

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure log file encryption	**logging file encryption** **alogrithms SMV4 key** *password*	Optional By default, the log file in Flash is not encrypted

9.2.7 Configure Log Display Colors *-B -S -E -A*

Configuration Conditions

None

Configure Log Display Colors

When log information is displayed, you can modify log information of different levels so that they are displayed in different colors. In this way, the importance degrees of logs are distinguished. By default, the log display color function is enabled. The following table shows the default colors corresponding to the log levels.

Table 9-13 Description of System Log Colors

Field	**Description**
emergencies	Red
alerts	Purple
critical	Blue
errors	Brown
warnings	Cyan

notifications	White
informational	Green
debugging	Green

Table 9-14 Configuring Log Display Colors

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure a color for logs of a level.	**logging color** [*logging-level* [*logging-color*]]	Optional. By default, each log level has a corresponding log display color.

NOTE

- If the control console or monitor console needs to output log information in different colors, you need to configure the color option of the terminals; otherwise, no color is displayed for the log information.

9.2.8 System Log Monitoring and Maintaining *-B -S -E -A*

Table 9-15 System Log Monitoring and Maintaining

Command	Description
clear logging [**buffer** | **file**]	Clear log information of the device.
clear logging syslog [**buffer** | **file**]	Clears log information that is collected when the device acts as the log server.
show logging [**buffer** | **file**]	Display the log information that is stored in the memory or flash memory.
show logging filter	Display the filtration configuration of logs.

Command	Description
show logging [**syslog**] **message-counter**	Display the size of log files and number of log records.
show logging syslog [**file**]	Display the logs that are stored in the flash memory.
show logging time / level	Display logs according to the log level or log time range.

10 Software Upgrade

10.1 Overview

Software upgrade provides a more stable software version and more abundant software features for the user.

Upgraded programs are stored in the storage mediums of the device in the form of files or data blocks. The software modules with different functions cooperate to keep the device in the stable working state and support the hardware features of the device and application services of users.

Users can upgrade software through the TFTP/FTP network transmission mode or the Xmodem transmission mode of the Console port. In upgrading software of different types, users must carefully read the operation steps and notes and cautions described in the manuals related to the software upgrade.

In upgrading software, you usually need to upgrade software of each type. If the software of a type is not updated during the upgrade process, you need not upgrade the software again. Usually, you can restart the device only after the all software versions are upgraded.

The following types of software are available:

- The image program package: Program package with the suffix pck. It contains a group of programs that are required for normal operation of the system, including operating system and application programs.
- The bootloader program: Program with the suffix bin. It is similar to the BIOS program of the PC which is frozen into the ROM of the main board. It is the first to be executed when the system is powered on. The program initializes the basic system, and realizes the functions such as upgrading, downloading, booting, commissioning, and testing. The bootloader program of the main control board and the switching board can be upgraded.

10.2 Software Upgrade Function Configuration

Table 10-1 Software Upgrade Function List

Configuration Tasks	
Upgrade the image program package.	Upgrade the image program package in TFTP/FTP mode.
Upgrade the bootloader program.	Upgrade the bootloader program in TFTP/FTP mode.

Configuration Tasks	
	Upgrade the bootloader program through the Console port.

10.2.1 Upgrade the image Program Package *-B -S -E -A*

Configuration Conditions

Before upgrading the image program package, ensure that:

- The route between the TFTP/FTP server and the device interface is reachable, and the TFTP/FTP server and the device can ping each other successfully.
- The TFTP/FTP server configuration is correct, and the image program is stored in the specified directory of the TFTP/FTP server.
- The remaining space of the flash memory is sufficient. If the space is insufficient, manually delete files that are not in use.
- The configuration files have been backed up.

Upgrade the image Program Package in TFTP/FTP Mode

Enter the privileged user mode, ensure that the device can obtain the upgrade program through the external TFTP/FTP server, and then use the **sysupdate image** command to upgrade the program package.

Table 10-2 Upgrading the image Program Package in TFTP/FTP Mode

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Upgrade the image program package.	**sysupdate image mpu** [**vrf** *vrf-name*] *dest-ip-address filename* [**ftp** *ftp-username ftp-password*] [**reload**]	Mandatory. If the FTP option is not specified, TFTP is used for upgrade by default.

Example: The following example shows how to make use of the FTP server 130.255.168.45 to upgrade the image program package with the image file name sp3-g-6.5.1(2).pck through the device interface.

```
Hostname#sysupdate image mpu 130.255.168.45 sp3-g-6.5.1(2).pck ftp a a
Hostname#sysupdate image mpu 130.255.168.45 sp4-g-6.5.0(46).pck ftp a a
```

#The device gives the following prompt messages:

```
downloading "sp3-g-6.5.1(2).pck" : ################(omitted#)###################OK
Download "sp3-g-6.5.1(2).pck" (6562832 Bytes) successfully

Verify the image...valid!
Not enough space for new version in /flash,
          please insure enough space for system upgrade.
```

```
Do you want to delete /flash/sp4-g-6.5.0(25).pck file?(y/n)yes
Writing file /flash/sp3-g-6.5.1(2).pck ............ (Omitted)...................OK!
backup ios to raw flash........ .. .................. (Omitted)...................OK!

Sysupdate image sp3-g-6.5.1(2).pck successfully
```

#The above message indicates that the image program of the device has been upgraded successfully.

NOTE

- If the command option reload is added, the system prompts whether to save the configuration and whether to restart the device. However, usually the device is started after all programs are upgraded. Therefore, the reload option is not recommended.
- Before the upgrade, ensure that there is sufficient space in the flash memory. If the space is insufficient, the upgrade fails. In this case, you can manually delete files that are not in need from the flash memory to obtain more space for upgrading application programs.
- It takes a long time to upgrade the image program package. A smaller remaining space in the flash memory results in longer upgrade time.
- After the upgrade is completed, to run the new image program, restart the device.
- If the device fails to start normally, open the bootloader screen, modify the startup mode to network startup. After the device is started successfully, start the upgrade. For the method, refer to the related section in the bootloader configuration manual and command manual.

Warning

- During the upgrade process, the device must not be powered off or restarted. Otherwise, the system may fail to start, or the flash file system of the main control board may be damaged.

10.2.2 Upgrade bootloader *-B -S -E -A*

Configuration Conditions

The following tasks have to be completed prior to the upgrading of the bootloader program:

- The routing reachability of TFTP/FTP server and Device ports are ensured and can be pinged from each other.
- The TFTP/FTP server is properly configured and the bootloader program is properly stored under designated directory of the TFTP/FTP server;
- The configuration file is backed up.

Upgrading the bootloader Program in TFTP/FTP Mode

Enter privilege user mode, make sure the Device can get upgrade program from external TFTP/FTP server and then be upgraded with the sysupdate bootloader command.

Table 10–3 Upgrading the bootloader Program in TFTP/FTP Mode

Steps	Command	Description
Enter privilege user mode	None	Required
Upgrade bootloader program	**sysupdate bootloader [device {***memberId* **| all}] mpu [vrf** *vrf-name***]** *dest-ip-address filename* [**ftp** *ftp-username ftp-password*] [**reload**]	Required If no FTP option has been specified, upgrade in TFTP mode is used by default

For example: in stacking mode, upgrade the bootloader program with an upgrade file named sz03-tboots1-rtk93-1.0.0.10.pck from FTP server 130.255.168.45.

```
Hostname# sysupdate bootloader device all mpu 128.255.21.170 sz03-tboots1-rtk93-1.0.0.10.pck ftp a
123456

# The Device would prompt the following message:

checking "sz03-tboots1-rtk93-1.0.0.10.pck" : ...OK

downloading "sz03-tboots1-rtk93-1.0.0.10.pck" : ##OK

Download "sz03-tboots1-rtk93-1.0.0.10.pck" (1849684 Bytes) successfully


Sysupdate start to write bootloader sz03-tboots1-rtk93-1.0.0.10.pck:

Update bootloader start.............OK.

Bootloader write successfully.

 %Sysupdate bootloader is in process, please wait...

%Sysupdate bootloader finished...


        sysupdate bootloader result information list:

-----------------------------------------------------------------

        Card                result information

-----------------------------------------------------------------

        Device 0 - Mpu       sysupdate successfully!
```

# The above information shows that the Device's bootloader has been successfully upgraded, and the upgrade result report and log information will be exported upon completion of the upgrade.

NOTE

- If the command option reload is appended, then a prompt will appear asking whether or not to save the configuration and whether or not to reload the Device immediately. Generally the Device is restarted on the condition that various programs have been upgraded. Therefore, the option reload is not recommended in general conditions.

- Upon completion of an upgrade, if it is necessary to run the new bootloader, the Device has to be restarted.
- Please choose the correct bootloader version for the upgrade in order to prevent abnormalities from happening.

Warning

- During the upgrade process, make sure that the Device is never powered off or restarted; otherwise, the system may be failed to start and the Device's bootloader may be damaged.

Upgrade the bootloader through via the Console Port

Make sure the HyperTerminal can access the Device via the Console Port and enter bootloader mode; adjust baud rate and upgrade the bootloader via the HyperTerminal's ymodem.

The detailed descriptions of the specific command, please refer to relevant chapters of the bootloader's command manual.

Table 10–4 Upgrade the bootloader through via the Console Port

Steps	Command	Description
Set up HyperTerminal	None	Required Run the HyperTerminal program, choose corresponding serial port (e.g., com1) and set up its attributes: set the baud rate to 9600 bps, enable software flow control, set the number of data bit to 8; there should be and 1 stop bit and no parity check bit.
Enter bootloader mode	None	Required During the restart of the Device, press CTRL+C to enter bootloader mode
Change the baud rate of the Console Port and the HyperTerminal to speed up upgrade	**srate** { *speed* }	Optional Change the Device's Console Port's baud rate to 115200bps, then disconnect the

Steps	Command	Description
		HyperTerminal, change the baud rate of the HyperTerminal to 115200bps and reconnect.
Upgrade bootloader program	**mupdate bootloader**	Required In bootloader mode, enter the bootloader command, then choose the HyperTerminal's y modem protocol, select the bootloader program and start the transmission

For example: upgrade the bootloader of the main master control card via the Console Port.

```
# The Device would prompt the following message:
RTL9310# # mupdate bootloader
Download bootloader start...
## Ready for binary (ymodem) download to 0x80000000 at 9600 bps...
CCC
Starting ymodem transfer.  Press Ctrl+C to cancel.
Transferring sz03-tboots1-rtk9310-1.0.0.10.bin...
  100%     904 KB     872 bytes/sec 00:17:41       0 Errors



## Total Size      = 0x000e2130 = 926000 Bytes
Download bootloader OK.
  Loader Chip: 93100000
  Loader CRC: 98ba8309
  Loader Size: e2058
  Loader Tail CRC: 85eed660
Program flash start...
1048576 bytes written, 0 bytes skipped
Program flash OK.
Update bootloader OK.
RTL9310# #
```

# The above information indicates that the Device's bootloader has been successfully upgraded.

NOTE

- When upgrading the bootloader, make sure the HyperTerminal's baud rate is identical to the baud rate of the Device's Console Port.
- When upgrading the bootloader, it is recommended that the transmission rate value be set to 115200bps in order to shorten the transmission time for the upgrade.
- If the Console Port's default rate has been changed during the upgrading of the bootloader, then the Device's Console Port's rate will automatically be restored to 9600bps when loading the image program package. In such circumstances, the HyperTerminal's rate has to be changed synchronously.
- It is recommended that the bootloader be upgraded via TFTP/FTP mode if possible. If not, the bootloader can be upgraded using the Console Port.

NOTE

- During the upgrade process, make sure the Device is not powered off, otherwise the system may not be able to start and the Device's bootloader file may be damaged.

10.2.3 Upgrade the Package File -B -S -E -A

The package file contains image and bootloader files and can be used to upgrade these files in one go.

Configuration Preparation

The following tasks have to be completed prior to the upgrading of the package file:

- The routing reachability of TFTP/FTP server and Device ports are ensured and can be pinged from each other.
- The TFTP/FTP server is properly configured and the package file is properly stored under designated directory of the TFTP/FTP server;
- The configuration file is backed up.

Upgrading the Package File in TFTP/FTP Mode

Enter privilege user mode, make sure the Device can get upgrade program from external TFTP/FTP server and then be upgraded with the sysupdate package command.

Table 10–5 Upgrading the Package File in TFTP/FTP Mode

Steps	Command	Description
Enter privilege user mode	None	Required

Steps	Command	Description
Upgrade package file	**sysupdate package [vrf** *vrf-name***]** *dest-ip-address filename* [**ftp** *ftp-username ftp-password* **][no-comparision][reload]**	Required If no FTP option has been specified, upgrade in TFTP mode is used by default

# Use FTP server 130.255.168.45 to upgrade the Device's sp35-g-9.4.0.17(R)-001.pkg file.

```
Hostname# sysupdate package 130.255.168.45 sp35-g-9.4.0.17(R)-001.pkg FTP a a
```

NOTE

- If the command option reload is appended, then a prompt will appear asking whether or not to save the configuration and whether or not to reload the Device immediately. Generally the Device is restarted on the condition that various programs have been upgraded. Therefore, the option reload is not recommended in general conditions.

Warning

- Make sure the Device is not powered off during the upgrade process, otherwise the system may not be able to start properly and the files may be damaged.

10.3 Typical Configuration Example of Software Upgrade

10.3.1 Upgrade Software Version *-B -S -E -A*

Network Requirements

- The PC is used as the FTP server, the Device is used as the FTP client; the server and Device are connected via network.
- On the • FTP server, set the user name with which the Device log on to the FTP server to admin and the password to admin; place the upgrade package program to be upgraded under the FTP server's directory to comprehensively upgrade all software application versions that support package upgrade on the Device.

Network Topology

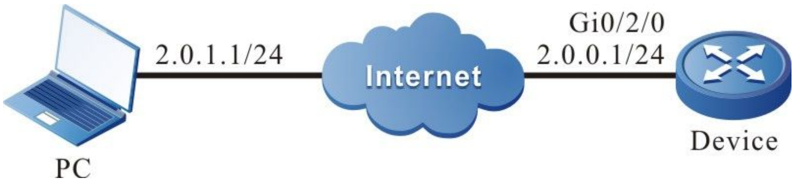


Figure 10-1 Networking Diagram - Package Upgrade of All Supported Software Versions

Configuration Steps

Step 1: Configure the FTP server, and place the package upgrade program under the FTP server's directory. (omitted)

Step 2: Backup Device configuration file. (omitted)

Step 3: Configure interfaces' IP addresses, so that the Device is connected to the FTP server via network. (omitted)

Step 4: Upgrade package upgrade program.

# Use sysupdate to upgrade package upgrade program.

```
Device#sysupdate package device all 128.255.21.170 sp35-g-9.4.0.12(R)-001.pkg ftp a 123456 no-comparision
```

A list of the upgrade results will be printed upon completion of the upgrade for the user to determine the upgrade results of all upgrade programs contained in the upgrade package file.

```
    package sysupdate result information list:
---------------------------------------------------------------


sysupdate sp35-g-9.4.0.12(R).pck result information list:
---------------------------------------------------------------
    Card            result information
---------------------------------------------------------------
    Device 0 - Mpu      device is not online,skipped!
    Device 1 - Mpu      device is not online,skipped!
    Device 2 - Mpu      device is not online,skipped!
    Device 3 - Mpu      device is not online,skipped!
    Device 4 - Mpu      sysupdate successfully!
    Device 5 - Mpu      device is not online,skipped!
    Device 6 - Mpu      device is not online,skipped!
    Device 7 - Mpu      device is not online,skipped!


sysupdate sz03-tboots2-rtk93-1.0.0.10.pck result information list:
---------------------------------------------------------------
    Card            result information
```

```
-----------------------------------------------------------------
       Device 0 - Mpu      device is not online,skipped!
       Device 1 - Mpu      device is not online,skipped!
       Device 2 - Mpu      device is not online,skipped!
       Device 3 - Mpu      device is not online,skipped!
       Device 4 - Mpu      sysupdate successfully!
       Device 5 - Mpu      device is not online,skipped!
       Device 6 - Mpu      device is not online,skipped!
       Device 7 - Mpu      device is not online,skipped!
```

NOTE

- Prior to the package upgrade, please make sure all cards are in place and in Start OK status. During the upgrade process, please do not plug in/pull out cards. Otherwise, the cards may experience abnormality in upgrade and may fail to start afterwards.

NOTE

- If the parameter no-comparision is selected, no comparison of image version will be carried out and the versions in the upgrade package will be directly used for upgrade of programs. If the parameter is not selected, the versions of image will be compared. If the version of image in the upgrade package is lower than or equal to the current version on the Device, then the Device will prompt the user and wait for the user to confirm whether or not to upgrade to the image upgrade program in the upgrade package. Whether the user chooses to upgrade the program or not, the upgrade of other upgrade files in the upgrade package will not be affected. If the upgrade package contains only the image file and the user choose not to upgrade, then the package upgrade will end.
- The command can also be appended the parameter “reload”. If the parameter is appended, the Device will be restarted directly upon the completion of the upgrade.

Step 5: Command restart Device

# Use reload command to reboot the Device.

```
Device #reload
Save current configuration to startup-config(Yes|No)?y
Please confirm system to reload(Yes|No)?y
```

It is up to the user to decide whether or not to save the configuration prior to restart.

NOTE

- If the upgrade command contains “reload” parameter, then this step can be omitted.

Step 6: Check the result.

# When the upgrade is completed and the Device is restarted, use show package version can check the version information of the files upgraded by the upgrade package.

```
Device #show package version

package       :sp35-g-9.4.0.12(R)-001.pkg

image        :sp35-g-9.4.0.12(R).pck

bootloader     :sz03-tboots2-rtk93-1.0.0.10.pck
```

# Use show system version brief can check the version number of the programs to see whether they have been upgraded.

```
Device #show system version brief

Device 4:

Module              Online State     Name                  BootLoader  IOS              CMM PCB CPLD FPGA

----------------------------------------------------------------------------------------------------------------

member device 4 Mpu 0 online Start Ok  MTS2848-6X-E 1.0.0.10    9.4.0.12(integrity) /   001 /    /
```

NOTE

- Use show package version can check the version of upgrade files in the upgrade package, and use the corresponding show system version brief to see the final upgrade results.

10.3.2 Upgrade All Software Versions *-B -S -E -A*

Network Requirements

- A PC acts as an FTP server, and Device acts as an FTP client. The network between the server and the device is normal.
- On the FTP server, the user name for a device to log in to the FTP server is admin, and the password is admin. The image program and bootloader program to be upgraded are placed in the FTP server directory.

Network Topology

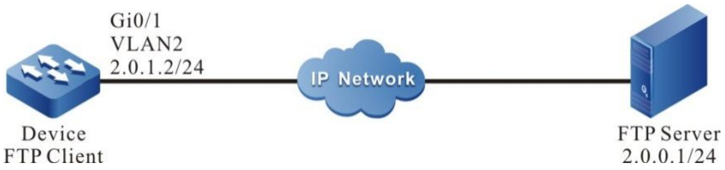


Figure 10-2 Networking for Upgrading All Software Versions

Configuration Steps

Step 1: Configure an FTP server, and place the image program and bootloader program in the FTP server directory. (Omitted)

Step 2: Back up device configuration files. (Omitted)

Step 3: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 4: Configure the IP addresses of the interfaces so that the network between Device and the FTP server is normal. (Omitted)

Step 5: Upgrade the image program.

#Before upgrading the image program, check whether there is sufficient space in the file system.

```
Device#filesystem
Device(config-fs)#volume
Device(config-fs)#exit
```

#Use the sysupdate command to upgrade the image program of the device.

```
Device#sysupdate image mpu 2.0.0.1 sp4-g-6.5.0(41).pck ftp admin admin
```

For the upgrade procedure of the image program and the print information which indicates whether the upgrade is successful, refer to the "Upgrading the image Program Package" in "Configuring Software Upgrade Functions".

Step 6: Upgrade the bootloader program.

#Use the sysupdate command to upgrade the bootloader program of the device.

```
Device#sysupdate bootloader mpu 2.0.0.1 MonitorIB005_V1.17.bin ftp admin admin
```

For the upgrade procedure of the bootloader program and the print information which indicates whether the upgrade is successful, refer to the "Upgrading the bootloader Program" in "Configuring Software Upgrade Functions".

Step 7: Use a command to restart the device.

#Use the **reload** command to restart the device.

```
Device #reload
Save current configuration to startup-config(Yes|No)?yes
Please confirm system to reload(Yes|No)?yes
```

Before the restart, determine whether to save the configuration according to the actual requirement.

Step 8: Check the result.

#After the upgrade is completed and the device is restarted, view the version numbers of the programs to check whether the versions have been upgraded.

#Check whether the image and bootloader programs have been upgraded successfully.

```
yyl_2948#sh system mpu

  System Card Information(Device:0 - Mpu 0 - ONLINE)
```

```
----------------------------------------------------------------
              Type:   SM2948-28TC(V1)[0x204e9381]
             Status:   Start Ok
          Last-Alarm:   Normal
        Card-Port-Num:   24
      Card-SubSlot-Num:   0
     Power-INTF-Status:   Normal
     Power-Card-Status:   On
          Serial No.:   6336134680200340
           Card-Name:   SM2948-28TC(V1)
         Description:
   Hardware-Information:
                    HW-State: 0
                  PCB-Version: 002
                 CPLD-Version: 101
   Software-Information:
              Monitor-Version: 1.28
             Software-Version: 6.6.3(5)(integrity)
Temperature-Information:
             Temperature-State:
                           Temperature = 51.C
                            Last-Alarm = Normal.
CPU-On-Card-Information:   < 1 CPUs>
                    CPU-Idx:  00
                     Status:  Normal
                    Core-Num:  0001
                  Core-State:
                    Core-Idx-00
                         Core-Status:  0000
                     Core-Utilization:  0%
                 Temperature:
                    Temperature-State:
                              Temperature = 65.C
                               Last-Alarm = Normal.
MEM-On-Card-Information:  <1 MEMs>
                    MEM-Idx:  00
                  MEM-State:
                        BytesFree =   94577228 bytes
                       BytesAlloc =  172574100 bytes
                       BlocksFree =        13 blocks
                      BlocksAlloc =      5839 blocks
                  MaxBlockSizeFree =   27262976 bytes
                        SizeTotal =  267151328 bytes
DISK-On-Card-Information:
                    DISK-Idx:  00
                       Type:  Flash
                     Status:  Online
                  DISK-State:
                      SizeTotal =   20728320 bytes
                       SizeFree =    4190208 bytes
      CMM-Information:
              Monitor-Version: 1.0.3
             Software-Version: 1.0.3
----------------------------------------------------------------

STATISTICS:       1 IN, 0 OUT, 0 IERR, 0 OERR
```

NOTE

- It does not matter whether the image program or the bootloader program is upgraded first, but the device can be restarted only after all programs have been upgraded.
- Before the upgrade, ensure that there is sufficient space in the flash file system for saving the image file that is used for upgrade. If there is not sufficient space on the device, delete the files that are not in need from the file system of the device. The remaining space of

the flash file space is recommended to be larger than 7M before the upgrade.

- If some programs are not updated in the newly released version, the unchanged programs need not be upgraded.

10.3.3 Upgrade the bootloader Program via the Console Port *-B -S -E -A*

Network Requirements

- PC and the Console port of the device are directly connected.
- The bootloader program is to be upgraded through the Console port.

Network Topology

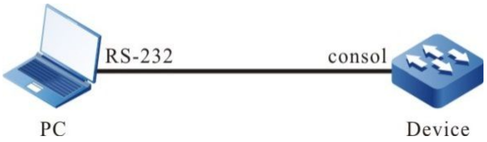


Figure 10-3 Upgrading the bootloader Program via the Console Port

Configuration Steps

Step 1: Connect PC and the Console port of the device properly. (Omitted)

Step 2: Open the bootloader screen.

When the device is just started and the "bootloader version 1.17 is Booting (press ctrl+c to enter bootloader mode)" message is printed, press and hold **Ctrl + C** to open the bootloader screen.

Step 3: Set the transmission rate to 115200 bps to improve the upgrade speed.

```
Monitor:> srate 115200
```

#After setting the transmission speed of the Console port of bootloader, you should set the transmission speed of the HyperTerminal also to 115200 bps.

Step 4: On the bootloader screen, upgrade the bootloader version.

```
Monitor:>lxr
```

#Input the **lxr** command, and use Xmodem to transmit the bootloader file that has been saved on the PC.

#Check the result.

#After the upgrade is completed, the following message is printed under the bootloader screen.

```
download success, image size = 0x80000 ( 524288 )
Update bootloader flash.
```

Step 5: Check the result.

#After the upgrade is completed and the device is restarted, the system is booted by the new bootloader, and the following message is printed:

```
bootloader  version 1.17 is Booting (press ctrl+c to enter  bootloader mode) .....
Now start loading system and application programs,
Loading system and application programs, please wait for a while...
```

NOTE

- Upgrade through the Console port is complex and slow, so the TFTP/FTP upgrade mode is recommended. The Console port upgrade mode is used only when the upgrade conditions of the TFTP/FTP upgrade mode fail to be satisfied.
- After the upgrade is completed, use the **reset** command to exit bootloader program. Then, the new bootloader program boots the loading of the image program.
- If the default rate of the Console port has been modified in upgrading the bootloader program, in loading the image program package, the rate of the device Console port automatically resumes to 9600 bps. At this time, the rate of the HyperTerminal needs to be modified synchronously.

11 Bootloader

11.1 Overview

In an embedded system, bootloader runs before the Operating System (OS) kernel runs. bootloader is used to initialize hardware devices (including the Console port, Ethernet port, and flash), and set up memory space mapping to bring the hardware and software of the system to a proper state. Finally, it prepares a proper environment for booting the OS kernel. In the embedded system, there is no such firmware program as BIOS, so the booting of the entire system is implemented by the bootloader.

The bootloader system mainly provides the following functions:

- Sets startup parameter to load and run the specified image program, and sets the mode in which the image program is loaded.
- Clears system configuration files of the device.
- Upgrades the bootloader program.
- Formats the flash file system of the device.

11.2 Configure bootloader Functions

Table 11-1 bootloader Function List

Configuration Tasks	
Set the bootloader startup parameters.	Set the bootloader startup parameters.
Clear system configuration files of the device.	Clears system configuration files of the device.
Upgrade the bootloader program.	Upgrade the bootloader program.
Format the flash file system of the device.	Format the flash file system of the device.

11.2.1 Preparation before Configuring the bootloader Functions *-B -S -E -A*

Before configuring the bootloader functions, you need to set up a local configuration environment. Connect the serial port of the host (or terminal) to the Console port of the device through a configuration cable. The configuration of the communication parameters of the host (or terminal) must be the same as the default configuration of the Console port of the device. The default configuration of the Console port of the device is as follows:

- Transmission speed: 9600 bps
- Flow control mode: None
- Check mode: None
- Stop bit: 1 bit
- Data bit: 8 bits

11.2.2 Enter bootloader Configuration Mode *-B -S -E -A*

Configuration Conditions

None

Enter bootloader Configuration Mode

Table 11–2 Enter bootloader Configuration Mode

Steps	Command	Description
Enter bootloader configuration mode	None	Required When the Device is powered on, press “ctrl+c” will enter the bootloader configuration mode; a message prompting “RTL93xx#” will appear upon entry of the mode.

NOTE

- In bootloader configuration mode, functions available in bootloader mode can be executed.

11.2.3 Set the bootloader Startup Parameters *-B -S -E -A*

Configuration Conditions

None

Set the bootloader Startup Parameters

Table 11-2 Setting the bootloader Startup Parameters

Step	Command	Description
Enter the bootloader configuration mode.	None	Mandatory. After the device is powered on, press the Ctrl + C keys to enter the bootloader configuration mode. After you enter the mode, the "bootloader :>" is prompted.
Set the bootloader startup parameters.	**change** [*index*]	Mandatory. By default, bootloader startup parameters with the index 0 are set.

NOTE

- If the device startup type is set to system startup, you can select the same of an existing image program from the flash file system for loading and operation according to the prompt message.
- If the device startup mode is set to network startup, after configuring startup parameter, first you need to ensure that the route from the Ethernet interface of the host or terminal and the network management interface (such as netdrv0) of the device is reachable. To check whether the network connection is normal, ping the IP address of the device from the host. In addition, ensure that the FTP server configuration of the host is correct, that is, the login user name and password that are configured on the device must be the same as those configured on the FTP server.

11.2.4 Upgrade the bootloader Program *-B -S -E -A*

Configuration Conditions

None

Upgrade the bootloader Program

Table 11-3 Upgrading the bootloader Program

Step	Command	Description
Enter the bootloader configuration mode.	None	Mandatory. After the device is powered on, press the Ctrl + C keys to enter the bootloader configuration mode. After you enter the mode, the "bootloader :>" is prompted.
Set the working speed of the Console port.	**srate** *speed*	Mandatory. The default working speed of the Console port is 9600 bps. To improve the efficiency in upgrading the bootloader system program, it is recommended that you set the working speed of the Console port to 115200 bps.
Upgrade the bootloader program.	**lxroot**	Mandatory.

NOTE

- The bootloader system program adopts the dual backup mode, that is, the main bootloader program and the backup bootloader program form a backup. The **lxroot** command upgrades only the main bootloader program, while the backup bootloader program keeps unchanged.
- After modifying the working speed of the device Console port, you need also configure the transmission speed of the serial port of the host (or terminal) to the same speed.
- After upgrading the bootloader system program, run the **reset** command or power off and restart the device. Then the new bootloader system program is used. After the device is restarted, the working speed of the Console port resumes the default speed 9600 bps.
- It is not recommended that you upgrade the bootloader program with the **lxroot** command. After the image program is loaded and it runs completely, use the **sysupdate** command to upgrade the bootloader program. This upgrade mode is more efficient than upgrade in the bootloader environment.

11.2.5 bootloader Monitoring and Maintaining *-B -S -E -A*

Table 11-5 bootloader Monitoring and Maintaining

Command	Description
version	Display bootloader program's version number.
print *index[0~4]*	Display the information of the startup parameters specified by the index.

11.3 Typical Configuration Example of bootloader

11.3.1 Configure bootloader to Boot the Image Program from the Network *-B -S -E -A*

Network Requirements

None

Network Topology

None

Configuration Steps

#Input the **change** command to set startup parameters with index 0 for bootloader.

```
bootloader:>change 0
```

#According to the prompt message, select to boot the Image program from the network management interface netdrvo of the device.

```
Please change the system boot parameters with the following operation:
'.' = clear field;  '-' = go to previous field;  ^D = quit

available boot devices:
 netdrv0 flash0(devname: '/flash')

boot device          : netdrv0
```

#Input the Image program file name sp3-g-6.5.0.4.1.pck.

```
file name            : sp3-g-6.5.0.4.1.pck
```

#Set the IP address of the network management interface netdrv0 to 192.168.0.2.

```
local IP addr        : 192.168.0.2
```

#Set the IP address of the FTP server of the host to 192.168.0.1.

```
host IP addr         : 192.168.0.1
```

#Do not set the gateway IP address.

```
gateway IP addr      :
```

#Set the user name for logging into the FTP server to admin.

```
user name            : amdin
```

#Set the password for logging into the FTP server to admin.

```
ftp password         : amdin
```

#Save the Image program to the flash file system.

```
save Image           : 1
```

#Input the **run** command to start booting the Image program.

```
bootloader:>run
```

12 PoE Management

12.1 Overview

The existing Ethernet, with its basic structure of Cat.5 cabling unchanged, not only transmits data signals for IP-based terminals (such as IP phones, WLAN access points, and network cameras), but also provides the DC power supply for the devices. This technology is called Power over Ethernet (PoE). The PoE technology ensures not only the security of existing structured cabling but also normal operation of the existing network, greatly reducing the cost.

PoE is also called Power over LAN (PoL) or Active Ethernet. It is the latest standard specification for making use of existing standard Ethernet transmission cable to transmit data and provide power. It is compatible with the existing Ethernet systems and users. IEEE 802.3af and IEEE802.3at are the technical standards that PoE must comply with. IEEE802.3af is the basic standard of the PoE technology. It is based on the IEEE 802.3, and the standards related to direct power supply through network cables are added. It is an extension of the existing Ethernet standards. IEEE802.3at is an extension based on the IEEE802.3af.

According to the definition of the IEEE802.3af standard, a complete PoE power supply system consists of two types of devices: Power Sourcing Equipment (PSE) and Power Device (PD).

- PSE: It provides power to other devices.
- PD: Devices that receive power. The power of the devices is usually not large.

12.1.1 PSE/PD Interface Specifications *-S -E -A*

For the 10BASE-T and 100BASE-TX IEEE802.3af networks, IEEE802.3af defines Power Interfaces (PIs), which are interfaces between PSE/PD and network cables. Currently, it has defined two power supply modes, Alternative A (signal wire pairs) and Alternative B (signal wire pairs 4, 5, 7, and 8). The following is a description of the two power supply modes:

1. Power supply through signal wire pairs (Alternative A)

As shown in the following figure, a PSE can supply power to a PD through signal wire pairs. Because DC and data frequency does not interfere with each other, electric current and data can be transmitted through the same wire pair. For electric cables, this is a kind of "multiplexing". Wires 1 and 2 are connected to form a positive (or negative) polarity, and wires 3 and 6 are connected to form a negative (or positive) polarity.

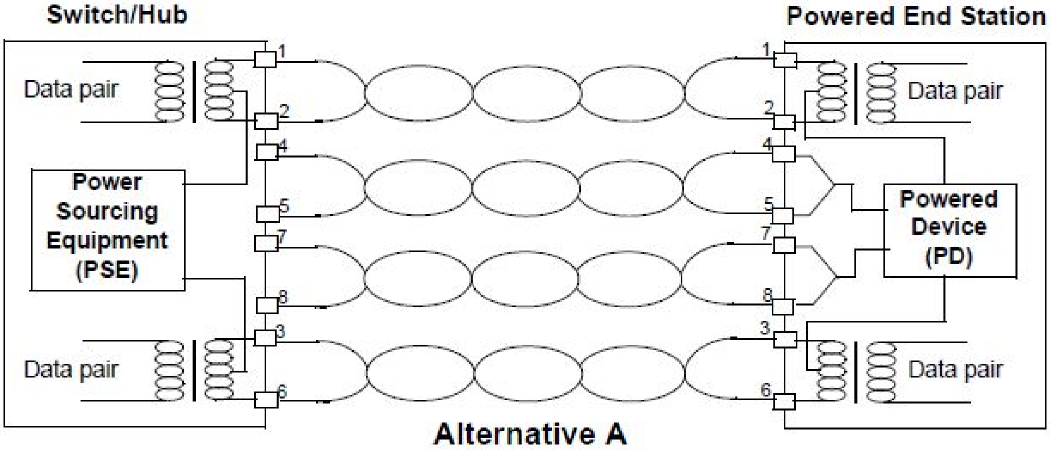


Figure 12-1 Alternative A Power Supply Mode with 10BASE-T and 100BASE-TX

2. Power supply through idle wire pairs (Alternative B)

As shown in the following figure, a PSE can supply power to a PD through idle wire pairs. Wires 4 and 5 are connected to form a positive polarity, and wires 7 and 8 are connected to form a negative polarity.

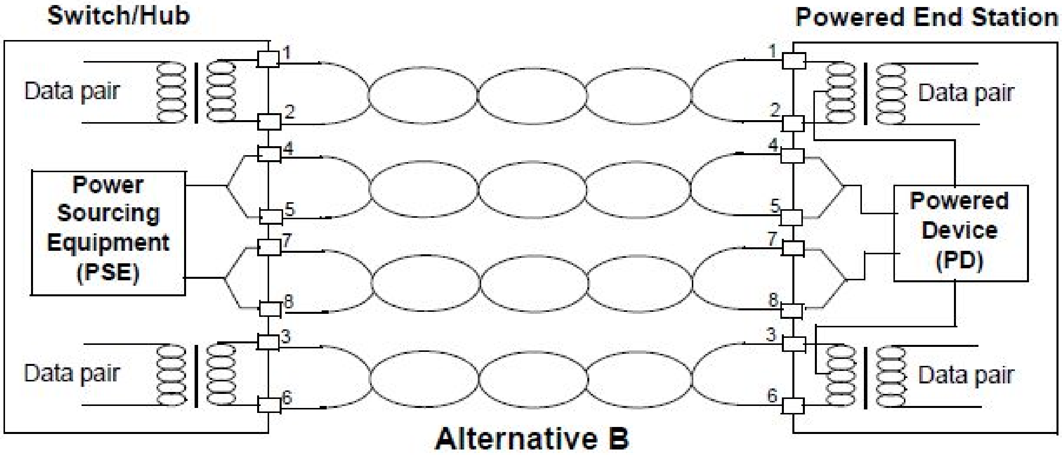


Figure 12-2 Alternative B Power Supply Mode with 10BASE-T and 100BASE-TX

According to IEEE802.3af, standard PDs must support both power supply through signal wire pairs and power supply through idle wire pairs, while PSEs need only support either of the two modes.

12.1.2 PoE Power Supply Process *-S -E -A*

If a PSE is installed in a network, the PoE Ethernet power supply process is as follows:

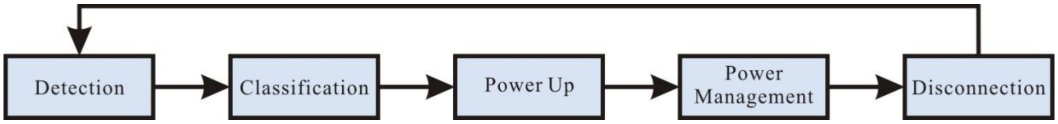


Figure 12-3 PSE Power Supply Process

- Detection: After a network device is connected to a PSE, the PSE first detects whether the device is a PD to ensure that the current is not supplied to non-PDs because supplying power to a device that is not a PD may damage the device. The PSE detects the resistance capacitance between the power output wire pairs to determine whether PDs exist. The PSE proceeds to the next step only after it detects PDs.
- Classification: After detecting PDs, the PSE classifies the PDs. It determines power grade of PDs by detecting power output current. During the power supply process, classification is optional.
- Power Up: Within a startup period which is configurable (usually less than 15 us), the PSE starts to provides low power voltage to PDs and gradually increases the power voltage to 48 V DC.
- Power Management: The PSE provides stable and reliable 48 V DC power for PDs. Once the PSE starts to supply power, it continuously detects PD current inputs. If the current consumption of a PD drops under the minimum value owing to various causes, such as the PD is disconnected, the PD encounters power consumption overload or short circuit, and the power load exceeds the PSE power supply load, the PSE regards the PD as not in position or abnormal. In this case, the PSE stops providing power to the PD.
- Disconnection: The PSE detects the current of PDs to determine whether PDs are disconnected. If a PD is disconnected, the PSE stop supplying power to the PD quickly (usually within 300 to 400 ms), and then the PSE returns to the Detection status.

12.2 PoE Function Configuration

Table 12-1 PoE Function List

Configuration Tasks	
Configure PoE basic functions.	Enable the global PoE function.
	Enable the interface PoE function.
	Enable the forced power supply function of an interface.
Configure the PoE power.	Configure the total power of PoE.
	Configure the protection power of PoE.
	Configure the maximum output power limit mode of an interface.

Configuration Tasks	
	Configure the maximum output power of an interface.
Configure power supply priorities.	Configure a PoE power management mode.
	Configure the power supply priority of an interface.
Configure PD power-on parameters.	Configure the PD detection mode of an interface.
	Configure the interface classification mode.
	Configure the power-on impulse current mode of an interface.
Configure the abnormality recovery function.	Configure the time for recovery from a power supply abnormality of an interface.
	Restart the PoE power supply.

12.2.1 PoE Basic Function Configuration *-S -E -A*

The PoE function is controlled by configuring global PoE and interface PoE, that is, the PoE function can be used only when the global PoE and interface PoE are both enabled. If you run the command for disabling the global PoE, the PoE functions of all interfaces are disabled. If you run the command for disabling the interface PoE function, you can choose to disable the PoE function of some interfaces. The interface PoE function is a standard power supply mode, while the interface forced power supply function is a special power supply mode. You can select only one mode at a time. However, both of the two modes are valid only after the global PoE function is enabled.

Configuration Conditions

None

Enable the Global PoE Function

Table 12-2 Enabling the Global PoE Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the global PoE function.	**power enable**	Optional.

Step	Command	Description
		By default, the global PoE function is enabled.

Enable the Interface PoE Function

Table 12-3 Enabling the Interface PoE Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the global PoE function.	**power enable**	Optional. By default, the global PoE function is enabled.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Enable the interface PoE function.	**power enable**	Optional. By default, the interface PoE function is enabled.

Enable the Forced Power Supply Function of an Interface

Table 12-4 Enabling the Forced Power Supply Function of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the global PoE function.	**power enable**	Optional. By default, the global PoE function is enabled.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Enable the forced power supply function of an interface.	**power force** { **always** | **once** }	Mandatory. By default, the forced power supply function of an interface is disabled.

NOTE

- Forced power supply is a special power supply mode, which does not require enabling the interface PoE function.

12.2.2 Configure the PoE Power *-S -E -A*

Configuration Conditions

Before configuring the PoE power, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure the Total Power of PoE

By configuring the total power of PoE, you can limit maximum output power of the device. If the total power required by all PDs exceeds the configured total power, power supply to some PDs is stopped according to the current power supply priority mode.

Table 12-5 Configuring the Total Power of PoE

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the total power of PoE.	**power total-power** *power-value*	Optional. By default, the total power is the maximum total power that the device power supply can provide.

Configure the Protection Power of PoE

When a PD is normally powered, the consumed power fluctuates within a certain range. To prevent PD power-off owing to power fluctuation, part of power is reserved from the total power of the device to act as the protection power. When the consumed power of the PD increases, the increased part is allocated from the protection power.

Protection power may also be allocated as normal power supply. When the available power is insufficient for providing power to newly connected PDs, if the available power of the device and the protection power is equal to or larger than the maximum output power of the interface of the new PD, sufficient power is allocated from the protection power to the new PD.

Table 12-6 Configuring the Protection Power of PoE

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the protection power of PoE.	**power guard-band** *guard-band-value*	Optional. By default, the protection power of the power supply is 40.0 watt.

Configure the Maximum Output Power Limit Mode of an Interface

The maximum output power of an interface is determined by the PD classification type. You can also customize the maximum output power of an interface.

Table 12-7 Configuring the Maximum Output Power Limit Mode of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the maximum output power limit mode of an interface.	**power threshold-mode** { **classification** | **user** }	Optional. By default, the maximum output power limit mode is the user customization mode.

Configure the Maximum Output Power of an Interface

You can limit the maximum power that a PSE can supply to a PD through an interface. If the power required by a PD exceeds the maximum output power of the interface, the PSE stops power supply to it.

Table 12-8 Configuring the Maximum Output Power of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-

Step	Command	Description
Configure the maximum output power limit mode to the user customization mode.	**power threshold-mode user**	Mandatory. By default, the maximum output power limit mode is the user customization mode.
Configure the maximum output power of an interface.	**power port-max-power** *max-power-value*	Optional. By default, the maximum output power is 30.0 watt.

12.2.3 Configure Power Supply Priorities *-S -E -A*

With the power supply priority function, if the total power of a PSE is insufficient for powering all PDs, key PDs have the priority to obtain power. Through this function, you can configure the mode in which key PDs are powered.

Configuration Conditions

Before configuring power supply priorities, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure a PoE Power Management Mode

Table 12-9 Configuring a PoE Power Management Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure PoE power management mode.	**power manage** { **dynamic-fifs** | **dynamic-priority** }	Optional. The default power management mode is the dynamic First In First Served (FIFS).

Configure the Power Supply Priority of an Interface

If the PoE power management mode is the dynamic priority mode, when the power supply of the PSE is insufficient, the PD that is connected to the interface with a higher power supply priority is first powered. If the power supply priorities of the interfaces are the same, the PD that is connected to the interface with smaller number is powered first.

Table 12-10 Configuring the Power Supply Priority of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the PoE power management to dynamic priority.	**power manage dynamic-priority**	Optional. The default power management mode is the dynamic priority.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the power supply priority of an interface.	**power priority** { **critical | high | medium | low** }	Optional. The default power supply priority is low.

12.2.4 Configure PD Power-On Parameters *-S -E -A*

PoE power-on process falls into the following stages:

1. Detection: The PSE detects whether PDs exist.
2. Classification: The PSE grades PDs and determines power consumption of PDs. This stage is optional.
3. Power-Up: The PSE supplies power to PDs.

You can adjust the parameters set for the previous stages and supply power to PDs of different types.

Configuration Conditions

Before configuring PD power-on parameters, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure the PD Detection Mode of an Interface

After the PoE function of an interface is enabled, the PSE detects the resistance capacitance between the power output wire pairs to determine whether PDs exist. The standard detection mode detects only PDs that comply with IEEE802.3af and IEEE802.3at. The standards define PDs and non-PDs, but there is a type of devices with resistance capacitance between those of PDs and non-PDs. The compatible mode can detect this type of devices.

Table 12-11 Configuring the PD Detection Mode of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the PD detection mode of an interface.	**power detect-mode** { **compatible** | **standard** }	Optional. The default PD detection mode is the standard mode.

Configure the Interface Classification Mode

After the interface PoE function is enabled, the PSE detects the output current of the power supply to determine the power grades of PDs. Power is allocated to PDs according to the power grades of the PDs. PD classification is an optional step. You can skip the step by setting the non-classification mode.

Table 12-12 Configuring the Interface Classification Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the interface classification mode.	**power class-mode** { **standard** | **never** }	Optional. By default, no classification is support.

NOTE

- Some non-standard PDs may not support classification. In this situation, the PD is classified to class0 by default, and the maximum output power of the interface is 15.4 watt.

Configure the Power-On Impulse Current Mode of an Interface

The PoE standard defines the PD power-on impulse current. The parameter is related to PSE, (parasitic) capacitance of the PD, and power of the PD. For the PDs that comply or not comply with the standard, the required power-on impulse current may be different. For different PDs, the related power-on impulse current mode must be configured.

Table 12-13 Configuring the Power-On Impulse Current Mode of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the power-on impulse current mode of an interface.	**power power-up-mode** { **802.3af | high | Pre-802.3at | 802.3at** }	Optional. The default power-on current mode is high.

12.2.5 Configure the Abnormality Recovery Function *-S -E -A*

When there is a PoE power supply abnormality, the abnormality recovery function is supported, including automatic recovery and manual recovery.

Configuration Conditions

Before configuring the abnormality recovery function, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure the Time for Recovery from a Power Supply Abnormality of an Interface

If a PSE detects abnormal power supply status of an interface while powering PDs, it automatically disables the PoE function of the interface. After the time for recovery from a power supply abnormality elapsed, it enables the PoE function again, and tries to supply power to the PD of the interface.

Table 12-14 Configuring the Time for Recovery from a Power Supply Abnormality of an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the time for recovery from a power supply abnormality of an interface.	**power recover-time** *time-value*	Optional. By default, the time for recovery from a power supply abnormality is 0

Step	Command	Description
		minute, indicating recovery immediately.

Restart the PoE Power Supply

When a PoE power supply abnormality occurs or the PoE power supply is abnormal, you can manually hot restart the PoE power supply to try to recover from the abnormal status.

Table 12-15 Configuring the Time for Recovery from a Power Supply Abnormality of an Interface

Step	Command	Description
Restart the PoE power supply.	**power reload**	Mandatory.

NOTE

- During the power supply restart process, if you run the power reload command again, the system prompts command execution failure.

12.2.6 Configure PoE Alarm Threshold Value *-S -E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of PoE:

- Enable global PoE function;
- Enable interface PoE function.

Configure PoE Alarm Threshold Value

When PoE is equal to or less than the set power threshold, a Trap alarm prompt will be sent.

Table 12-16 Configure PoE Alarm Threshold Value

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure PoE alarm threshold value	**power alarm-threshold** { **all** | *system-id* { **all** |	Optional

Steps	Command	Description
	subsystem-id } } *threshold-value*	By default, the power supply's power alarm threshold value is 99%

12.2.7 PoE Monitoring and Maintaining ***-S -E -A***

Table 12-17 PoE Monitoring and Maintaining

Command	**Description**
show power { **manage** | **summary** | **configure interface** *interface-name* | **detect interface** *interface-name* | **pd-status interface** *interface-name* | **version** }	Display the PoE configuration and the power supply status information.

13 LUM

13.1 LUM Overview

LUM: Local User Manager(LUM) is a local user database for providing aaa local authentication.

RBAC: Role Based Access Control(RBAC) by establishing the association between “authority<->role” endows authority to a role and by establishing the association between “role<->user” assigns a role to the user so that the user gets the authority for corresponding role. The basic idea of RBAC is to assign a role to the user and the assigned role defines the system functions and resources objects to which the user is permitted to operate.

The separation of authority and user provides RBAC with the following merits:

• The administrator does not have to assigned authorities to users one by one. Instead, he/she only has to predefine roles with corresponding authorities and then assign a role to the user. Therefore, RBAC adapts to the change of user better and improves the flexibility in user authority assignment.

• Since the relations between roles and users change frequently but the relations between roles and authorities are relatively stable, this stable correlation can be used to reduce the complexity of user authorization management and cut down management expenses.

Roles: sets of rules.

Rules: the permit/deny authorities of commands with specified features or all features.

Features: modules.

13.2 LUM Function Configuration

Table 13-1 LUM Function Configuration List

Configuration task	
Configure user role	Configure user role
Configure administrator scheme	Configure administrator

Configuration task	
	Configure administrator user group
Configure access user scheme	Configure access user
	Configure user group

13.2.1 Configure Roles -B -S -E -A

By default there are four roles, i.e., Security-admin, Network-admin, Audit-admin and Network-operator, whose authorities cannot be changed.

The authorities of custom roles are subsets of those of Network-admin. They are not permitted to configure the modular authorities that have been endowed to Security-admin/Audit-admin. Their specific authorities are as shown in the following table.

	Log	History	User management/user authentication	Other modules
Public	NO	NO	Change their own password	Show running, exit, etc.
Security administrator	Commands for checking and configuring operation log	History configuration and operation	OK	lai module, line, service, AAA
Audit-admin	Commands for checking and configuring data log	NO	NO	NO
Network-admin	All commands other than those for operation log and data log	History configuration and operation	NO	OK
Network-operator	All show commands within the authorities of Network-admin	show commands	NO	All show commands within the authorities of Network-admin

By default, user has not been configured with any role attribute. When the attributes of a user's role take effect, the user's grade is invalidated; the user's role supersedes the user's grade and becomes the basic criteria for command authorization: the user depending on his/her role has different authorities to execute different commands.

Configuration Conditions

None

Configure User Role

Table 13-2 Configure User Role

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create a user role and enter the user role mode	**role** *role-name*	Required By default there are four roles, i.e., Security-admin, Network-admin, Audit-admin and Network-operator, whose authorities cannot be changed.
Create a rule for the user role	**rule** *number* **{ deny | permit } feature {all |** *feature-name* }	By default, there is no rule defined for newly created user roles, i.e., current user role does not have any authority. Revision of rules takes no effect on current online users but will take effect on users who log in to use their roles. Rules with smaller ID number have higher priority level

13.2.2 Configure Local User -B -S -E -A

Local users are stored on the Device: including local administrators and local access users. It only takes effect when the authentication mode is local. When a Local User is created, it will be specified as an administrator or an access user.

Configuration Conditions

None

Configure Local Administrator User

Table 13-3 Configure Administrator

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create administrator user and enter administrator user mode	**local-user** *user-name* **class manager**	Required. By default, administrator user is not configured.

Configure Local Access User

Table 13-4 Configure Access User

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create access user and enter access user mode	**local-user** *user-name* **class network**	Required. By default, access user is not configured.

13.2.3 Configure Administrator User's Attributes *-B -S -E -A*

Administrator refers to a user that log on to the Device.

When configuring the user attributes of local administrators, the following configuration limits and guidances apply:

- If a user has been designated a role by AAA authorization at times of login, then whether a command is to be executed when the user log on to the Device shall depend on the user's role; if the user has not be designated a role by AAA authorization at times of login, then whether a command is to be executed when the user log on to the Device shall depend on the user's grade.

- For SSH users, if no authentication mode has been configured in user view for log on to the Device with public key authentication, the commands available to the user are identical to the commands available to their user roles or user grades (user roles have higher priority level than user grades) as configured in the view of the local administrator user who has the same name with the SSH users. For more detailed introduction to user roles, please refer to “Configure roles” in “LUM Configuration Guide”.
- User attribute "maximum authentication tries" can be configured either in local administrator user view or administrator user view. The configuration priority levels in descending order for the configuration views are:local administrator user view-->administrator user group view.
- User attribute "life cycle of password" can be configured either in local administrator user view or administrator user view. The configuration priority levels in descending order for the configuration views are:local administrator user view-->administrator user group view-->global view.

Configuration Conditions

None

Configure Administrator User's Attributes

Table 13-5 Configure Administrator

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create administrator user and enter administrator user mode	**local-user** *user-name* **class manager**	Required. By default, no administrator user is created.
Configure administrator user's password	**password 0** *password*	Required. In default state, the user has no password.
Set up the server type(s) that can be used by the user	**service-type { ssh | telnet | console | ftp | web}**	Required. In default state, the user does not support any service-type
Set up to user role to which the Local User belongs	**user-role** *role-name*	Optional. By default, administrator role is not configured.

Steps	Command	Description
		The administrator role has a priority level higher than the administrator level, in other words, if an administrator user has been configured a role, the administrator's authority shall be that for the administrator's role.
Set up the user group to which the administrator belongs	**group** *group-name*	Optional. By default, no user group has been configured.
Configure the authorization grade of the login user	**privilege** *privilege-level-number*	Optional. By default, the user grade is 1
Configure the command to be automatically executed by the user	**autocommand** *command-line*	Optional. By default, no command has been configured for a user to execute automatically.
Configure the option command(s) to be automatically executed by the user	**autocommand-option** { **nohangup** [**delay** *delay-time-number*] |**delay** *delay-time-number* [**nohangup**] }	Optional. By default, the Device is disconnected upon the completion of the automatic execution of command(s) and the time delay for automatic execution of command(s) is 0.
Configure the life cycle of the user	**password-control livetime** *user-live-time*	Optional. By default, life cycle of user is not limited
Configure the maximum number of login attempts	**password-control max-try-time** *max-try-time-number*	Optional. By default, user management will not limit

Steps	Command	Description
for administrator users		the maximum number of tries.
Configure the maximum number of online users of the same group.	**max-online-num** *user-number*	Optional. By default, there is no limit on the maximum number of online users of the same group.
Configure users' authority to access files	**filesys-control{read | write | execute | none}**	Optional. By default, users have permissions to read, write, and/or execute files.
Configure the Device directory available for administrators to access or manage	**work-directory** *directory*	Optional. By default, the directory is /flash. Presently the attribute is for configuring the file directory for ftp users to log on to the Device.

13.2.4 Configure the Attributes of Access Users -B -S -E -A

Access users are users who access the network via the Device.

Configuration Conditions

None

Configure Access User

Table 13-6 Configure Access User

Steps	Command	Description
Enter global configuration mode	**configure terminal**	
Create access user and enter access user mode	**local-user** *user-name* **class network**	Required. In default state, no access user has been configured.

Steps	Command	Description
Configure access user's password	**password 0** *password*	Required. In default state, the user may not be able to log on to the Device if the user has no password.
Set up the server type(s) that can be used by the access user	**service-type** { **xauth }**	Required. In default state, the user does not support any service-type
Set up the user group to which the access user belongs	**group** *group-name*	Optional. In default state, no user group has been configured to which the access user belongs.
Configure user status	**stat** { **active / block** }	Optional. By default, user status is active.

13.2.5 Configure Local User Group -B -S -E -A

Local Users can be divided into administrator user group and access user group.

Administrator user group, the set of administrator user attributes, supports the configuration of the life cycle of password and the maximum number of login attempts.

Access user group are for managing access users, it has nested hierarchy for more visualized reflection of a company or department's organizational structure relationship. For the time being, access user group does not support any attribute of access users.

Configuration Conditions

None

Configure Administrator User Group

Table 13-7 Configure Administrator User Group

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create administrator user	**manager-group** *group-name*	Required.

Steps	Command	Description
group and enter its mode		By default, no administrator user group has been configured.
Configure the life cycle of password of users in administrator user group	**password-control livetime** *user-live-time*	Optional. By default, there is no limitation on the life cycle of administrator users in that user group, which means the life cycle of passwords is mainly configured in administrator user view.
Configure the maximum number of login attempts for users in administrator user group	**password-control max-try-time** *max-try-time-number*	Optional. By default, there is no limitation on the maximum number of login attempts for users in administrator user group, that is, the allowable maximum number of login attempts is mainly configured in administrator user view.

Configure Access User Group

Table 13-8 Configure Access User Group

Steps	Command	Description
Enter global configuration mode	**configure terminal**	
Create an access user group and enter its mode	**user-group** *group-name*	Required. By default, access user group has not been configured.
Configure the parent group of the access user's group	**parent** *group-name*	Optional. By default, the parent group is the parent path of the group name's path.

13.2.6 Configure Password Strategy -B -S -E -A

Our system has been designed with powerful password security strategy. The security of password is guaranteed from the perspectives of password complexity, force user to change password at first login and maximum number of login attempts. Password security strategies apply only to local administrator users.

Password complexity:

(1) With the minimum password length policy, the administrator can specify the minimum length of administrator user password. When setting user password, if the length of the entered password is shorter than the pre-set minimum length, the system will reject the password and prompt: "Bad password:it is too short."

(2) With the password combination test function, the administrator can define the combination types of the component elements of user password. The component elements of passwords consist of the following 4 types:

- Capital letters: [A~Z]
- Small letters: [a~z]
- Decimal numbers: [0~9]
- 31 special characters (`~!@$%^&*()_+-={}[]|\:;”’<>,./’)

4 combination types of password elements are allowed, which are specified as follows:

- Combination type 1: the password shall consist of at least 1 types of elements;
- Combination type 2: the password shall consist of at least 2 types of elements;
- Combination type 3: the password shall consist of at least 3 types of elements;
- Combination type 4: the password shall consist of all 4 types of elements;

When the user sets a password, the system will check whether the set password meets the configuration requirements. Only passwords that meet the requirements are accepted.

(3) The password shall not be identical to the user name. When setting administrator password, if the entered password is identical to the user name, the system will reject the password.

Force user to change password at first login:

When the function Force user to change password at first login is enabled, the system will display a message prompting users to change their password when they log on to the Device for the first time, otherwise they will be denied access to the Device. For the administrator user whose account name is “admin”, the system will force him/her to change his/her password before allowing the user to log on to the Device, regardless of whether the function Force user to change password at first login is enabled or not.

Life cycle of password:

Life cycle of password is used to limit the life of user password. When a password's life span is expired, the user will be required to change his/her password. If a user enters an expired password to log in, the system will prompt that the password is expired and the user has to reset his/her password in order to continue his/her local login. If the entered password does not meet the requirements, or the new passwords do not match, the system will deny access. For login modes that are not interactive, such as

FTP login, if the life span of a password is expired, the user can log on to the server only with a password changed by the administrator. If the login time period coincides with the expiry date of the password, the current login operation will be allowed, but the next FTP command will trigger desynchronization. In particular, if the user's first login coincides with the expiry of the password, the system will require the user to change password only once at login.

Maximum authentication tries:

The limit on maximum authentication tries is for preventing brutal force attack by malicious users. When the allowable maximum authentication tries are exceeded, the system will add the user name into the blacklist of the login-secure module and the user account will be locked out for a period of time.

Configuration Conditions

None

Configuration Conditions

Table 13-9 Configure Password Strategy

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure password complexity	**password-control complexity** {**min-length** *len*| **with user-name-check | composition type-number** *type-number* }	Optional. By default, the allowable minimum length of user password is 6 characters, and the password shall consist of at least 2 combination types of elements and shall not be identical to the user name.
Configure Force user to change password at first login	**password-control firstmodify enable**	Optional. By default, user is not required to change password at first time login. For the administrator user whose account name is “admin”, the system will force him/her to change password at his/her first login even if the Force user to change password at first login option is not enabled.

Steps	Command	Description
Configure the life cycle of the user	**password-control livetime** *user-live-time*	Optional. By default, life cycle of user is not limited
Configure the maximum number of login attempts for administrator users	**password-control max-try-time** *max-try-time-number*	Optional. This command shall be configured in administrator user group view or administrator user view. By default, the maximum number of login attempts for users in administrator user group has not been configured, that is, the allowable maximum number of login attempts is mainly configured in administrator user view.

13.2.7 LUM Monitoring and Maintaining *-B -S -E -A*

Table 13-10 LUM Monitoring and Maintaining

Command	Description
debug user { manager | network}	Access user management's debug information
show users class { manager | network } [*username* **]**	Display user configuration information
show role [*rolename* **]**	Display the configuration information of all roles or designated role(s)

13.3 Example of LUM Typical Configuration

13.3.1 Configure Network-Admin User *-B -S -E -A*

Network Requirements

- Configure Network-admin user, verify that he/she has the authority of Network-admin.

Network Topology

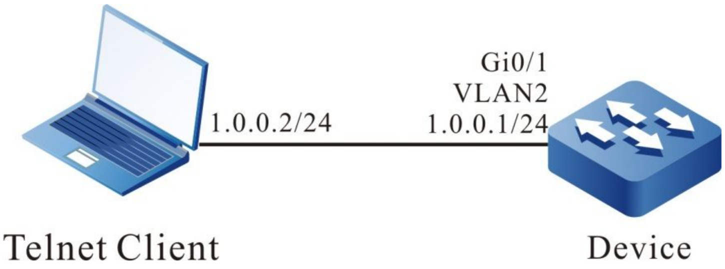


Figure 13-1 Networking Diagram - Configure Network-Admin User Group

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Configure administrator's attributes.

# Configure user admin and set password to admin.

```
Device#configure terminal
Device(config)#local-user admin class manager
Device(config-user-manager-admin)#password 0 admin
```

# Configure service type

```
Device(config-user-manager-admin)#service-type telnet ftp web console ssh
```

# Configure the user role of the local user as Network-admin

```
Device(config-user-manager-admin)#user-role network-admin
```

# Configure local authorization to activate the role

```
Device(config-user-manager-admin)#exit
Device(config)#domain system
Device(config-isp-system)#aaa authentication login local
Device(config-isp-system)#aaa authorization login local
Device(config-isp-system)#exit
```

# Configure for the use of login aaa authentication in line vty

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
```

Step 3: In Telnet client, enter the user name admin, and password admin to successful log on to the Device.

# Authenticated administrator user can execute administrator command show logging to view the log

```
Device#show logging
```

```
Logging source configurations
  console is enabled,level: 7(debugging)
  monitor is enabled,level: 7(debugging)
  buffer is enabled,level: 5(notifications)
  file is enabled,level: 7(debugging)
The Context of logging file:
```

```
# Authenticated Network-admin cannot execute other administrators' commands
Device#show role
You may not be authorized to perform this operation, please check.
```

NOTE

- By default, there are four administrator roles, i.e., security-admin, network-operator, audit-admin, and network-admin, which can be configured at discretion. Custom roles are also available for use.

14 Interface Basis

14.1 Overview

The interfaces supported by the device can be divided to physical interface and logical interface. The physical interface is Ethernet interface; logical interface includes aggregation group interface, VLAN interface, and so on.

Ethernet interface, also called L2 Ethernet interface or port, is one physical interface. It works in layer 2 in the OSI reference model-Data link layer and is mainly used for the data frame forwarding and MAC address learning.

Aggregation group interface is one logical interface, formed by binding multiple physical links between two devices. It also works at the data link layer and is mainly used to expand the link bandwidth and improve the link reliability.

VLAN interface is one logical interface, used to be bound with VLAN and complete the packet forwarding between different VLANs.

For different interfaces, there are corresponding configuration modes. The related configuration modes of the interfaces include:

- Interface configuration mode, corresponding to the VLAN interface
- L2 Ethernet interface configuration mode, corresponding to L2 Ethernet interface
- Aggregation group configuration mode, corresponding to aggregation group interface

This chapter mainly describes the common function configuration of various interfaces. For the featured function configuration of various interfaces, refer to the corresponding interface chapter.

14.2 Basic Function Configuration of Interfaces

Table 14-1 Basic Function Configuration List of Interfaces

Configuration Task	
Configure the basic functions of the interfaces	Enable/disable interface
	Configure interface description
	Configure the statistics interval of the interface traffic
Configure the interface group function	Configure interface group

14.2.1 Configure Basic Functions of Interfaces *-B -S -E -A*

Configuration Conditions

No

Enable/Disable Interface

After the port is disabled, it cannot receive or send packets, but after the port is enabled, whether it can receive and send packets also depends on other setting, such as whether the peer port is enabled, the rates of the local end and the peer port, whether duplex mode matches with MDIX (Media Dependent Interface Crossover).

After the aggregation group interface is disabled, all member ports are disabled; after the aggregation group interface is enabled, we can disable or enable one member port separately.

Table 14-2 Enable/Disable Interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either After entering the interface configuration mode, the subsequent configuration just takes effect on the current interface; after entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group interface; after entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	
Enable interface	**no shutdown**	Mandatory By default, the interface is enabled.
Disable interface	**shutdown**	Mandatory By default, the interface is enabled.

Configure Interface Description

The interface description is used for naming different interfaces, helping the user distinguish different interface types and actual service functions. It is convenient for the user to manage various interfaces.

Table 14-3 Configure Interface Description Information

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either After entering the interface configuration mode, the subsequent configuration just takes effect on the current interface; after entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group interface; after entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	
Configure interface description information	**description** *description-name*	Mandatory By default, the description information of the interface is not configured.

Configure Statistics Interval of Interface Traffic

Different interfaces carry different service traffics. Adjusting the statistics interval of the interface traffic can help the user concern the history records of the interface traffic selectively, forecasting the future trend of the interface traffic more correctly. It is convenient for the user to analyze and adjust the bored services of the interface.

Table 14-4 Configure Statistics Interval of Interface Traffic

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Either After entering the interface configuration mode, the subsequent configuration just takes effect on the current interface; after entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group interface; after entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	
Configure the statistics interval of the interface traffic	**load-interval** *load-interval-value*	Mandatory By default, the statistics interval of the interface traffic is 300s.

14.2.2 Configure Interface Group Functions *-B -S -E -A*

Bind multiple interfaces as one interface group. Configuring various interface commands on the interface group is equivalent to configuring on all interfaces of the interface group, while it is not necessary to configure on each interface repeatedly. Display the information of one interface group is to display the information of all interfaces in the interface group.

Configuration Conditions

The interfaces covered by the interface group should already exist.

Configure Interface Group

Table 14-5 Configure Interface Group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create interface group in the list mode	**interface group** *group-id* **enum** *interface-name1 interface-name2* … *interface-nameN* [**point-to-point** | **multipoint**]	Mandatory By default, the interface group is not created.
Enter the global configuration mode	**exit**	-
Create interface group by specifying range mode	**interface group** *group-id* **range** *start-interface-name end-interface-name* [**point-to-point** | **multipoint**]	Mandatory By default, the interface group is not created.

NOTE

- The interface types in the interface group should be the same. The user can configure multiple interface groups as desired.
- The user can configure the commands supported by all types of interfaces in the interface group, but if the interfaces covered by the interface group do not support, the commands do not take effect and there may be no error prompt. Please check whether the commands take effect by viewing the configuration.
- If the interface group covers the logical interface and when the logical interface is deleted, the logical interface in the interface group is also deleted automatically.

14.2.3 Configure Interface Status of SNMP Proxy *-B -S -E -A*

Actually there are two levels of interface UP/DOWN status in the system, i.e., L2 link level and L3 protocol level, which can be seen using the command show ip interface brief. Generally the two statuses vary with the up/down of the physical interfaces; however, when keepalive gateway is configured at ethernet interface, the L3 protocol level's status will be controlled by keepalive test status.

If SNMP proxy function is enabled on the Device, then network management server can get the status information of the interface via public mib and, if SNMP Trap is enabled, send the interface status change information to network management server.

This functional command can be used to configure the hierarchy of interface status of interest to the SNMP proxy. By default, the hierarchy of interface status of interest to the SNMP proxy is the L2 link level; however, if the ethernet interface is configured keepalive gateway, it is necessary to configure the hierarchy of interface status of interest to the SNMP proxy to L3 protocol level in order to make the interface status displayed on the network management server consistent with the tested keepalive status. Therefore, in an environment where keepalive test is enabled (e.g., MSTP WAN line environment), it is recommended that link-status-care l3 be configured.

Configuration Conditions

None

Configure Interface Group

Table 14-6 Configure Interface Status of SNMP Proxy

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the hierarchy of interface status network management	**link-status-care** { **l2** | **l3** }	Required By default, the hierarchy of interface status of interest to SNMP proxy is L2 link level
Enter global configuration mode	**exit**	-

14.2.4 Basic Monitoring and Maintaining of Interfaces *-B -S -E -A*

Table 14-6 Basic Monitoring and Maintaining of Interfaces

Command	**Description**
clear interface group *group-id*	Clear the statistics information of all interfaces in the interface group
interface group *group-id* **display**	Display all interfaces contained by the current interface group
show interface group *group-id*	Display the information of all interfaces in the interface group

15 Ethernet Interface

15.1 Overview

Ethernet interface, also called L2 Ethernet interface or port, is one physical interface. It works at layer 2 in the OSI reference model-data link layer. It is mainly used to execute two basic operations:

1. Data frame forwarding: According to the MAC address (that is physical address) of the data frame, forward the data frame. Ethernet interface can only perform the L2 switching forwarding for the received packets, that is, can only receive and send the packets whose source IP and destination IP are at the same segment.
2. MAC address learning: Construct and maintain the MAC address table, used to support forwarding the data frames.

According to the maximum rate supported by the port, the port type can be divided to the following three:

Fastethernet: 100M port, can be abbreviated as Fa, such as fastethernet0/1 or Fa0/1;

Gigabitethernet: 1000M port, can be abbreviated as Gi, such as gigabitethernet0/25 or Gi0/25;

Tengigabitethernet: 10 Gigabit port, can be abbreviated as Te, such as tengigabitethernet1/1 or Te1/1.

According to the media type of the port, the port type can be divided to copper (electrical port) and fiber (optical port).

15.2 Ethernet Interface Function Configuration

Table 15-1 Function Configuration List of Ethernet Interface

Configuration Task	
Configure basic functions of port	Enter the L2 Ethernet interface configuration mode
	Enter the batch configuration mode of L2 Ethernet interface
	Configure port rate and duplex mode
	Configure port MDIX (Media Dependent Interface Crossover) mode
	Configure the port media type

Configuration Task	
	Configure port MTU (Maximum Transmission Unit)
	Configure head-of-line blocking
	Configure port flow control
	Configure delay time
	Configure auto energy-saving of the port
	Configure the energy efficient Ethernet function of the interface.
Configure the port detection function	Configure the status flap detection of the port
	Enable port loopback test
	Configure the cable detection
Configure storm suppression	Configure the storm suppression parameter
	Configure the action executed after the storm suppression
Configure the UNI/NNI attribute of the port	Configure the UNI/NNI attribute of the port
	Configure the uni port connectivity

15.2.1 Configure Basic Functions of Port *-B -S -E -A*

Configuration Conditions

No

Enter L2 Ethernet Interface Configuration Mode

To configure on the specified port, first enter the L2 Ethernet interface configuration mode of the port and then execute the corresponding configuration command.

Table 15-2 Enter the L2 Ethernet Interface Configuration Mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Mandatory

NOTE

- The naming rule of the port number is S/P (Slot/Port). Slot indicates the slot on the device, numbered from 0. If there is fixed port, slot 0 is reserved for the fixed port. The service slot is numbered from 1. Port indicates the physical port on the device or service card. The port on each device and service card is numbered from 1.
- The naming rule of the port name *interface-name* is port type + port number. For example, gigabitethernet0/1 indicates the fixed port numbered 1 and the type is GE port; tengigabitethernet1/2 indicates the port numbered 2 on the service slot numbered 1 and the type is 10 GE port.

Enter Batch Configuration Mode of L2 Ethernet Interface

When performing the same configuration on multiple ports, to improve the configuration efficiency and reduce the repeated steps, select entering the batch configuration mode of the L2 Ethernet interface, including the following three cases: single port, such as gigabitethernet 0/1; successive ports, using "-" to indicate one section of successive ports, such as gigabitethernet 0/3-0/5, indicating port 0/3, 0/4, 0/5; single port and successive ports, using comma to separate, such as "gigabitethernet 0/1, 0/3-0/4, 0/6", indicating port 0/1, 0/3, 0/4, 0/6.

Table 15-3 Enter the Batch Configuration Mode of the L2 Ethernet Interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the batch configuration mode of the L2 Ethernet interface	**interface** *interface-list*	Mandatory

Configure Port Rate and Duplex Mode

Setting the port rate includes two cases:

One is to set the fixed rate according to the port rate capability set. The optional parameters include **10** (10M), **100** (100M), **1000** (1000M), **10000** (10000M).

The other is to set the rate as auto (auto-negotiation), specifying that the rate is negotiated by the local end and the peer port.

Similarly, setting the port duplex mode includes two cases:

One is to set the duplex mode according to the capability set of the port duplex mode. The optional parameters include full (full-duplex mode), indicating that the port can send packets when receiving the packets; half (half-duplex mode), indicating that the port can only receive or send packets at one moment, but cannot perform at the same time;

The other is to set the duplex mode as auto (auto-negotiation), indicating that the duplex mode is negotiated automatically by the local end and the peer port.

Table 15-4 Configure the Rate and Duplex Mode of the Port

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the port rate	**speed** { **10 | 100 | 1000 | 10000 | auto** }	Mandatory By default, the rate is auto.
Configure the port duplex mode	**duplex** { **auto | full | duplex** }	Mandatory By default, the duplex mode is auto.

NOTE

- When the port is the 100M optical port, the supported rate is 100M and auto, and the supported duplex mode is auto and full-duplex mode; when the port is 1000M optical port, the supported rate is 100M, 1000M and auto, the supported duplex mode is auto and full-duplex mode; when the port is the 10 gigabit optical port, the supported rate is 1000M, 10000M and auto, and the supported duplex mode is auto and full-duplex mode.
- When the rate and duplex mode of two gigabit optical ports are set as auto, the rate got by auto negotiation is 1000M, not 10000M, but the duplex mode is auto.

Configure Port MDIX Mode

We can send and receive signals only after connecting the local end and the peer port. Therefore, the MDIX mode is used with connection cables.

The cables connecting ports are divided to two types: straight-through cable and crossover cable. To support the two types of cables, provide three kinds of MDIX modes: normal, cross and auto.

The optical port can only support straight-through cable. Therefore, MDIX mode can only be set as normal.

The electrical port is formed by eight pins. You can change the roles of the pins by setting the MDIX mode. When setting as normal, use pin 1 and 2 to send signals, and pin 3, 6 to receive signals; when setting as cross, use pin 1, 2 to receive signals, pin 3, 6 to send signals; when setting as auto, the local and peer electrical ports automatically negotiate the functions of the pins by connecting the cables.

When using the straight-through cable, the MDIX modes of the local and peer ports cannot be the same.

When using crossover cable, the MDIX modes of the local and peer ports should be the same or at least one is auto.

Table 15-5 Configure Port MDIX Mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the mode of receiving and sending signals via network cable	**mdix** { **auto | cross | normal** }	Mandatory By default, the MDIX mode of the electrical port is auto and the MDIX mode of the optical port is normal.

Configure Port Media Type

Switch to use the optical port or electrical port on the Combo port by configuring the port media type. The optical port and the corresponding electrical port cannot work at the same time. When specifying one type of ports on Combo port, the other type of ports are automatically disabled.

Table 15-6 Configure Port Media Type

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure port media type	**media-type** { **auto | copper | fiber | fiber-to-copper** }	Mandatory By default, the media type of the electrical port is copper; the media type of the optical port is fiber;

Step	Command	Description
		the media type of the Combo port is copper.

NOTE

- When switching the optical port and electrical port on the Combo port, the port configuration after switching, such as rate, duplex mode, and MDIX mode, are initialized to the default values.

Configure Port MTU

The MTU configured on the port takes effect at the same time for the ingress and egress packets, and the set values are the same. When the length of the received and sent packets exceeds the set value, the packets are dropped directly.

In contrast, the MTU configured on L3 Ethernet interface only takes effect for the egress packets. When the length of the sent packet exceeds the set value, the packet first performs the IP fragmenting, making the length of the fragmented packet not exceed the set value, and then send it out.

Table 15-7 Configure Port MTU

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure port MTU	**mtu** *mtu-value*	Mandatory By default, the port MTU is 1824 bytes.

Configure Head-of-Line Blocking

When the port is blocked and if the head-of-line blocking function is enabled, the packets causing the block are directly dropped; if the head-of-line blocking function is disabled, process the packets causing the block according to the configuration of the port flow control.

Table 15-8 Configure Head-of-Line Blocking

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure head-of-line blocking	**hol-blocking** { **enable** | **disable** }	Mandatory By default, the head-of-line blocking function of the port is enabled.

Configure Port Flow Control

When the sending or receiving buffer is full and if the duplex mode of the port is half-duplex, send the blocking signals back to the source end by the back pressure mode; if the duplex mode of the port is full-duplex mode, the port informs the source end to stop sending by the flow control mode.

Table 15-9 Configure Port Flow Control

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure port flow control	**flowcontrol** { **on** | **off** }	Mandatory By default, the flow control function of the port is disabled.

NOTE

- When enabling the flow control function, first disable the head-of-line blocking function; when enabling the head-of-line blocking function, enabling the flow control function cannot take effect.
- The local flow control can be realized only when the local and peer ends both enable the flow control function.

Configure Delay Time

When the port changes from Up to Down, first enter the set suppression time period and the switching of the port status is not felt by the system; and then after the set suppression time, report the port status change to the system. In this way, we can avoid the unnecessary running cost caused by the frequent switching of the ports status in short time.

Table 15-10 Configure Delay Time

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure delay time	**link-delay** *link-delay-value*	Mandatory By default, the delay report time of the port changing from Up to Down is 0, that is, disable the delay report function; when the port changes from Up to Down, report and process immediately.

Configure Port Auto Energy-Saving

When disabling or enabling port auto energy-saving, but not connecting cables, the port inside is always in the polling port state. To reduce the unnecessary energy consumption, automatically switch to the low energy consumption state when the port is idle by configuring the port auto energy-saving.

Table 15-11 Configure Port Auto Energy-Saving

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure port auto energy-saving	**auto-power-down enable**	Mandatory By default, the auto energy-saving function of the port is disabled.

Configure Port Energy Efficient Ethernet Function

When no data traffic passes, the inner port is always polling the port state. To reduce such unnecessary consumption, you can configure the interface energy efficient Ethernet function. When the interface is idle, it is automatically switched to the low energy state. When the data is normally transmitted, recover the power supply.

Table 15-12 Configure the Interface Automatic Energy Saving

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the interface energy saving Ethernet function	**energy-efficient-ethernet enable**	Optional By default, the energy efficient Ethernet function of the interface is disabled.

NOTE

- After the interfaces on the both sides of the cable are enabled with the energy efficient Ethernet function, the function can take effect.
- The optical interface does not support such energy efficient Ethernet function.
- The interface with the rate as 10 Mbps and with the duplex mode as any mode and the interface with the rate as 100 Mbps and the duplex mode not as the automatic negotiation mode do not support the energy efficient Ethernet function.

15.2.2 Configure Port Detection Function *-B -S -E -A*

Configure Port Status Flap Detection

When the port changes from Down to Up and if the port status flap detection is configured and it meets the detection condition, it is regarded that the status flap happens to the specified port or called Link-Flap and the port is automatically disabled and set as Error-Disabled.

Table 15-13 Configure Port Status Flap Detection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure port flap detection	**errdisable flap-setting cause link-flap max-**	Mandatory By default, the trigger condition of executing

Step	Command	Description
	flaps *max-flaps-number* **time** *time-value*	Link-Flap is: within 10s, the detected port becomes Up for at least 5 times.

NOTE

- When the port is disabled by the Link-Flap function and set as Error-Disabled and if it is necessary to recover automatically, you can configure the command **errdisable recovery cause** to set the above function.

Enable Port Loopback Test

When performing some troubleshooting, such as locating the port fault initially, you can enable the port loopback test function. The port enabled with the loopback test function cannot forward packets normally.

The port loopback test function includes internal loopback test and external loopback test.

During internal loopback test, change the internal receiving end and sending end of the specified port to make the packets sent by the port loopback in the device and received by the port. If the internal loopback test succeeds, it indicates that the port inside works normally.

During the external loopback test, first insert one self-loop cable on the port and the packets sent by the specified port return to the port via the self-loop cable and received by the port. If the external loopback test succeeds, it indicates that the port works normally.

Table 15-14 Enable Port Loopback Test

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Enable port loopback test	**loopback** { **internal | external** }	Mandatory By default, the port loopback test function is not enabled.

Configure Cable Detection

The cable detection function is for the twisted-pair connected to the port, detecting the status and length of the cable. The user can judge whether there is something wrong with the cable according to the check result.

Table 15-15 Configure Cable Detection

Step	Command	Description
Configure cable detection	**test cable-diagnostics interface** *interface-list*	Mandatory By default, do not perform the cable detection.

NOTE

- The cable detection function is not applicable to the optical port.

15.2.3 Configure Storm Suppression *-B -S -E -A*

Configure Storm Suppression Parameters

Limit the broadcast, multicast or unknown unicast traffic on the port by configuring the storm suppression parameters. When the broadcast, multicast or unknown unicast traffic on the port exceeds the set threshold, the system drops the excessive packets, so as to make the proportion of the broadcast, multicast or unknown unicast traffic on the port reduce to the limited range and ensure the normal running of the network services.

Table 15-16 Configure Storm Suppression Parameters

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure storm suppression parameters	**storm-control** { **broadcast** | **multicast** | **unicast** } { *percent-value* | **bps** *bps-value* | **pps** *pps-value* }	Mandatory By default, the port storm suppression parameters are not configured.

Configure Action Executed after Storm Suppression

When the storm is detected on the specified port and the storm suppression is enabled, you can select two policies to process the storms on the port:

One is to disable the port and send the alarm information of detecting storm and disabling the port to the configured log server via trap. In the mode, the port is disabled, so the port cannot receive the subsequent traffic and the storm on the port is removed at once.

The other is to send the alarm information of detecting storm to the configured log server via trap. In the mode, the port is enabled, so the port can receive the subsequent traffic and the storm on the port cannot be removed.

Table 15-17 Configure Action Executed after Storm Suppression

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the action executed after storm suppression	**storm-control action** { **shutdown** | **trap** | **logging** }	Mandatory By default, the action to be executed is logging after the interface detects the storm.

NOTE

- When the port is disabled by the storm suppression function and set as Error-Disabled and it is necessary to recover automatically, you can set the above function by configuring the command **errdisable recovery cause**.

15.2.4 Configure Port UNI/NNI Type *-B -S -E -A*

Configure Port UNI/NNI Type

Uni port is the connection port between the user device and network; nni port is the connection interface between networks. On one device, the nni port and uni port or nni ports are interconnected; uni ports are separated from each other.

Table 15-18 Configure Port UNI/NNI Attribute

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the UNI/NNI attribute of the port	**port-type** { **nni** | **uni** }	Mandatory By default, the UNI/NNI type of the port is nni.

Configure Connectivity of uni Port

By default, all uni ports of one device are separated from each other. However, to realize the intercommunication between the specified multiple uni ports, but not change the separation relation between these uni ports and other uni ports, you can configure the connectivity of the uni port.

When configuring the connectivity on the specified uni port, you can only set whether the uni port can forward packets to other uni ports, not affecting whether other uni ports can forward packets to the specified uni port. Therefore, to realize the intercommunication among multiple uni ports, you should configure as community on these uni ports respectively.

Table 15-19 Configure the Connectivity of uni Port

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the connectivity of uni port	**uni-isolate** { **community** | **isolated** }	Mandatory By default, the uni port cannot forward packets to other uni ports.

NOTE

- The command can only take effect on the uni port.

15.2.5 Configure the Basic Functions of L3 Ethernet Interface *-B -S -E -A*

Depending on the processing levels of datagrams by ethernet interface, the ethernet interface can operate at L2 mode or L3 mode. If the operation mode of the ethernet interface is set to L2 mode, then the interface can be used as an L2 ethernet interface; if the operation mode of the ethernet interface is set to L3 mode, then the interface can be used as an L3 ethernet interface and it plays a role equivalent to a VLAN interface.

Configuration Conditions

None

Configure L3 Ethernet Interface

Table 15-22 Configure L3 Ethernet Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2/L3 ethernet interface configuration mode	**interface** *interface-name*	-
Configure L3 ethernet interface	**no switchport**	Required By default, the ethernet interface operates in L2 mode and is used for an L2 ethernet interface

NOTE

- When the ethernet interface switches its operation mode, all configurations under the ethernet interface except for description, shutdown, speed, duplex, media-type, mdix, eee configurations will be restored to the default configurations for the new mode.
- When the ethernet interface is used as an L3 interface, please refer to Configuration of basic functions of VLAN interface for the configurations of the basic functions of the L3 ethernet interface.

15.2.6 Ethernet Interface Monitoring and Maintaining *-B -S -E -A*

Table 15-20 Ethernet Interface Monitoring and Maintaining

Command	**Description**
clear cable-diagnostics [**interface** *interface-list*]	Clear the cable check result information of the specified port

Command	Description
clear interface { *interface-list* | **switchport** } **statistics**	Clear the packet and traffic statistics information of the port
show cable-diagnostics [**global** | **interface** *interface-list*]	Display the cable Check the result information
show errdisable flap-values	Display the current setting of triggering executing Link-Flap function
show interface { *interface-list* | **switchport** [**brief**] }	Display all information or abstract information of the port
show interface *interface-list* **statistics**	Display the packet and traffic statistics information of the port
show interface switchport statistics [**packet | rate**]	Display the packet and traffic statistics information of all ports on the device
show optical { **all | interface** *interface-list* } [**detail**]	Display the information of the optical module inserted on the port
show port-type [*interface-list* | { **uni** | **nni** } [*interface-list*]]	Display the UNI/NNI attribute information of the port
show protocol-state interface *interface-name* **vlan** *vlan-id*	Display the STP of the specified port in the specified VLAN
show storm-control [*interface-list*]	Display the storm suppression setting of the specified port

15.3 Typical Configuration Example of Ethernet Interface

15.3.1 Configure Storm Suppression Function *-B -S -E -A*

Network Requirements

Configure the storm suppression function on the port of the device to suppress the broadcast, unknown unicast and multicast packets, realizing that PC2 can access Internet normally when PC1 sends lots of broadcast, unknown unicast and multicast packets.

Network Topology

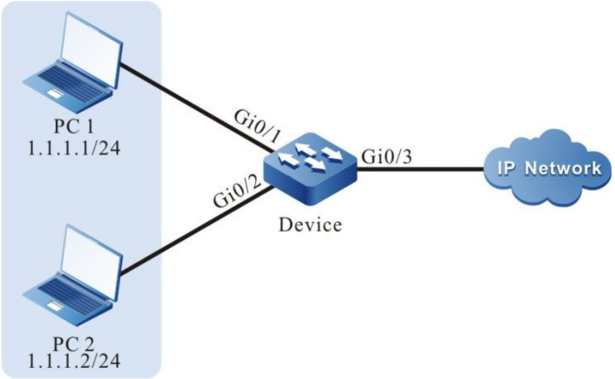


Figure 15-1 Network Topology of Configuring Storm Suppression

Configuration Steps

Step1: Configure VLAN and port link type on Device.

# Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/3 on Device as Trunk, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode trunk
Device(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/3)#exit
```

Step2: Configure the storm suppression function

#Adopt bps limitation mode to suppress the broadcast, unknown unicast and multicast packets on port gigabitethernet0/1 and the suppression rate is 1024Kbps.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#storm-control broadcast bps 1024
Device(config-if-gigabitethernet0/1)#storm-control unicast bps 1024
Device(config-if-gigabitethernet0/1)#storm-control multicast bps 1024
Device(config-if-gigabitethernet0/1)#exit
```

Step3: Check the result

#View the storm suppression information of port gigabitethernet0/1 on Device.

```
Device#show storm-control interface gigabitethernet 0/1
 Interface                  Unicast   Broadcast   Multicast   Action
 ------------------------------------------------------------------------
 gi0/1                     enable    enable     enable     none
```

#When PC1 sends lots of broadcast, unknown unicast and multicast packets, PC2 also can access Internet normally.

16 Aggregation Group Interface

16.1 Overview

Aggregation group interface is one logical interface. When enabling the link aggregation function on multiple ports, the multiple ports with the same link aggregation feature form the aggregation group and are abstracted to aggregation group interface; meanwhile, the multiple ports with the same attribute are called the member ports of the aggregation group. It is mainly used to expand the link bandwidth and improve the connection reliability.

16.2 Aggregation Group Interface Function Configuration

Table 16-1 Function Configuration List of Aggregation Group Interface

Configuration Task	
Configure the basic functions of the aggregation group interface	Enter the aggregation group configuration mode

16.2.1 Configure Basic Functions of Aggregation Group Interface *-B -S -E -A*

Configuration Conditions

No

Enter Aggregation Group Configuration Mode

Table 16-2 Enter the Aggregation Group Configuration Mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	Mandatory

NOTE

- Before entering the specified aggregation group configuration mode, first create the corresponding aggregation group.

16.2.2 Monitoring and Maintaining of Aggregation Group Interface *-B -S -E -A*

Table 16-3 Monitoring and Maintaining of Aggregation Group Interface

Command	Description
clear link-aggregation *link-aggregation-id* **statistics**	Clear the packet and traffic statistics information of the specified aggregation group
show link-aggregation [*link-aggregation-id* | **brief**]	Display all information of the aggregation group
show link-aggregation *link-aggregation-id* **statistics**	Display the packet and traffic statistics information of the specified aggregation group
show protocol-state link-aggregation *link-aggregation-id* **vlan** *vlan-id*	Display the STP (Spanning Tree Protocol) status of the specified aggregation group in the specified VLAN

17 VLAN Interface

17.1 Overview

VLAN interface is one logical interface, used to be bound with VLAN and complete the packet forwarding between different VLANs. One VLAN can only be bound to one VLAN interface. One VLAN interface also can only be bound with one VLAN.

17.2 VLAN Interface Function Configuration

Table 17-1 VLAN Interface Function Configuration List

Configuration Task	
Configure the basic functions of the VLAN interface	Configure VLAN interface
	Configure the logical bandwidth of the interface
	Configure interface delay
	Configure interface MTU

17.2.1 Configure Basic Functions of VLAN Interface *-B -S -E -A*

Configuration Conditions

No

Configure VLAN Interface

Table 17-2 Configure VLAN Interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create VLAN interface	**interface vlan** *vlan-id*	Mandatory By default, do not create VLAN interface.

NOTE

- VLAN interface is one logical interface. To work normally, you need to create the corresponding VLAN and add the physical port to VLAN. For how to create VLAN and add physical port to VLAN, refer to the VLAN chapter of the configuration manual.
- There is no order requirement for creating VLAN interface, creating VLAN and adding physical port to VLAN.

Configure Interface Logical Bandwidth

The logical bandwidth of the interface affects the calculation of the route cost and QoS, but does not affect the physical bandwidth of the interface. Usually, when the interface is connected to WAN, it is suggested that the logical bandwidth of the user configuration interface is consistent with the actual bandwidth of the leased line.

Table 17-3 Configure Interface Logical Bandwidth

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface vlan** *vlan-id*	-
Configure the logical bandwidth of VLAN interface	**bandwidth** *width-value*	Optional By default, the logical bandwidth of the VLAN interface is 100,000 Kbps.

Configure Interface Delay

The interface delay configuration affects the calculation of the routing protocol cost, but does not affect the actual transmission delay of the interface. The user can change the cost of the routing protocol by configuring the interface delay.

Table 17-4 Configure Interface Delay

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface vlan** *vlan-id*	-

Step	Command	Description
Configure VLAN interface delay	**delay** *delay-time*	Optional By default, the delay of the VLAN interface is 10 and the unit is 10 microsecond.

Configure Interface MTU

The interface MTU decides the maximum length of the IP fragment packet and the user can configure manually.

Table 17-5 Configure Interface MTU

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface vlan** *vlan-id*	-
Configure VLAN interface MTU	**mtu** *mtu-size*	Mandatory By default, the VLAN interface MTU is 1500 bytes.

17.2.2 VLAN Interface Monitoring and Maintaining *-B -S -E -A*

Table 17-6 VLAN Interface Monitoring and Maintaining

Command	Description
clear interface vlan *vlan-id*	Clear the statistics information of the specified VLAN interface
show interface vlan *vlan-id*	View the information of the specified VLAN interface
show interface vlan *vlan-id* **original statistics**	View the statistics information of the specified VLAN interface

17.3 Typical Configuration Example of VLAN Interface

17.3.1 Configure VLAN Interface *-B -S -E -A*

Network Requirements

Configure the VLAN interface on Device to realize the intercommunication between PC1 and PC2 of different VLANs.

Network Topology

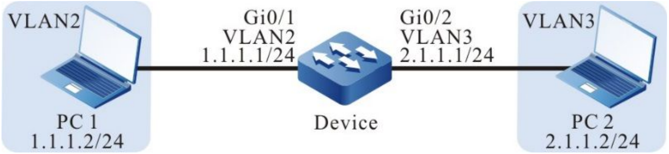


Figure 17-1 Network Topology of Configuring VLAN Interface

Configuration Steps

Step1: Configure VLAN and port link type on Device.

#Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device as Access. Port gigabitethernet0/1 permits the services of VLAN2 to pass and gigabitethernet0/2 permits the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 3
Device(config-if-gigabitethernet0/2)#exit
```

Step2: Configure the VLAN interface and IP address on Device.

#Create VLAN2 interface on Device whose IP address is 1.1.1.1 and subnet mask is 255.255.255.0; create VLAN3 interface whose IP address is 2.1.1.1 and subnet mask is 255.255.255.0.

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#ip address 1.1.1.1 255.255.255.0
Device(config-if-vlan2)#exit
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 2.1.1.1 255.255.255.0
Device(config-if-vlan3)#exit
```

Step3: Check the result.

#View the information of VLAN interface on Device.

```
Device#show interface vlan 2
vlan2:
    line protocol is up
    Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
    Type: ETHERNET_CSMACD
    Internet address: 1.1.1.1/24
    Broadcast address: 1.1.1.255
    Queue strategy: FIFO , Output queue: 0/1 (current/max packets)(0)
    Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Ethernet address is 0012.2355.9913
    5 minutes input rate 0 bits/sec, 0 packets/sec
    5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets received; 1 packets sent
    0 multicast packets received
    1 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
    Unknown protocol 0
Device#show interface vlan 3
vlan3:
    line protocol is up
    Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
    Type: ETHERNET_CSMACD
    Internet address: 2.1.1.1/24
    Broadcast address: 2.1.1.255
    Queue strategy: FIFO , Output queue: 0/1 (current/max packets)(0)
    Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
    Reliability 255/255, Txload 1/255, Rxload 1/255
    Ethernet address is 0012.2355.9913
    5 minutes input rate 0 bits/sec, 0 packets/sec
    5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets received; 1 packets sent
    0 multicast packets received
    1 multicast packets sent
    0 input errors; 0 output errors
    0 collisions; 0 dropped
    Unknown protocol 0
```

#PC1 can ping PC2.

18 Loopback Interface

18.1 Loopback Interface Overview

Loopback interface, also referred to as local loopback interface, is a logical virtual interface implemented by software. The interface is not affected by physical status and remains in enabled status so long as it is not manually closed. In dynamic routing protocols such as OSPF, the IP address of Loopback interface can be chosen for Router ID and Device identifier. The Device will deem all messages that are sent to the Loopback interface as messages sent to itself and will not forward such messages.

18.2 Configuration of Loopback Interface Function

Table 18-1 Functional Configuration List of Loopback Interface

Configuration task	
Configure the basic functions of Loopback interface	Configure the Loopback interface
	Configure the interface's logical bandwidth
	Configure interface time delay

18.2.1 Configure Basic Functions of Loopback Interface *-B -S -E -A*

Configuration Conditions

None

Configure the Loopback Interface

Table 18-2 Configure the Loopback Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create Loopback interface	**interface loopback** *unit – number*	Required

Steps	Command	Description
		By default, no Loopback interface is created

Configure the Interface's Logical Bandwidth

The interface's logical bandwidth will affect the calculation of routing cost consumption and QoS but will not affect the interface's physical bandwidth. Generally, when the interface is connected to a WAN, it is recommended that the user configure the interface's logical bandwidth to a value identical to the actual bandwidth of the leased line.

Table 18-3 Configure the Interface's Logical Bandwidth

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface's logical bandwidth	**bandwidth** *width-value*	Optional By default, the logical bandwidth of the Loopback interface is 8,000,000 Kbps

Configure Interface Time Delay

Interface time delay configuration will affect the calculation of protocol consumption but will not affect the interface's actual transmission time delay. The user can change the routing protocol's consumption by configuring interface time delay.

Table 18-4 Configure Interface Time Delay

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure interface time delay	**delay** *delay-time*	Optional By default, the time delay of Loopback interface is 5000 units of 10 microseconds

19 Null Interface

19.1 Null Interface Overview

Null interface is a logical virtual interface implemented by software. All messages sent to the Null interface will be discarded. Dynamic routing protocols such as OSPF will generate auto-summary routers, the outbound interface of which points to the Null interface. Thus, routing loop is effectively avoided. By default, Null0 interface is created by the Device and cannot be closed or deleted by user.

19.2 Configuration of Null Interface Functions

Table 19-1 Functional Configuration List of Null Interface

Configuration task	
Configure the basic functions of Null interface	Configure the basic functions of Null interface

19.2.1 Configure Basic Functions of Null Interface *-S -E -A*

Configuration Conditions

None

Configure Basic Functions of Null Interface

Table 19-2 Configure Basic Functions of Null Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter Null interface configuration mode	**interface null 0**	Required
Configure Prohibit sending ICMP unreachable error message	**no ip unreachables**	Optional

Steps	Command	Description
		By default, sending ICMP unreachable error message is prohibited.

NOTE

- Null interface only supports configuration for permitting or prohibiting the forwarding of ICMP unreachable error message.
- Messages arriving at Null interface will be discarded without forwarding ICMP unreachable error.

20 Virtualization Link Interface

20.1 Virtualization Link Interface Overview

A virtualization link interface is formed by bundling together multiple physical ports. A virtualization link interface is a logic link channel for internal protocol message exchange and transaction data forwarding between member switches in the stacking system. All physical ports in the virtualization link interface are known as its member ports.

The member switches join in the same switching domain and interconnect via the virtualization link interface to form a virtual switch.

20.2 Configuration of Virtualization Link Interface Functions

Table 7-1 Functional configuration List of Virtualization Link Interface

Configuration task	
Configure the functions of virtualization link interface	Enter virtualization link interface configuration mode

20.2.1 Configure the Functions of Virtualization Link Interface *-B -S -E -A*

Configuration Conditions

None

Enter Virtualization Link Interface Configuration Mode

Table 7-2 Enter Virtualization Link Interface Configuration Mode

Steps	Command	Description
Enter global configuration mode	configure terminal	-
Enter virtualization link interface configuration mode	vsl-channel *vsl-channel-id*	Required In single machine mode, *vsl-channel-id* is a one-dimensional value representing the virtualization link interface's number; in stacking mode, it is a two-dimensional value, the first dimension of which is the virtual member switch's number, the second dimension is the virtualization link interface's number

NOTE

- Before entering the virtualization link interface configuration mode, a corresponding virtualization link interface has to be created first.

20.2.2 Virtualization Link Interface Monitoring and Maintaining *-B -S -E -A*

Table 7-3 Virtualization Link Interface Monitoring and Maintaining

Command	Description
clear vsl-channel *vsl-channel-id* **statistics**	Clear designated virtualization link interface's message and network traffic statistics information

Command	Description
show vsl-channel *vsl-channel-id* **rate-peak** [**input** | **output**]	Display designated virtualization link interface's network traffic monitoring information
show vsl-channel *vsl-channel-id* **statistics**	Display designated virtualization link interface's message and network traffic statistics information

21 Link Aggregation

21.1 Overview

Through link aggregation, multiple physical links between two devices are bound to form a logic link so as to expand link capacity. Within the logic link, the physical links act as redundancy and dynamic backup of each other, providing higher network connection reliability.

21.1.1 Basic Concepts

Aggregation Group and Member Ports

Multiple physical ports are bound to form an aggregation group, and the physical ports are member ports of the aggregation group.

Member Port Status

The member ports of an aggregation group have the following two statuses:

- Selected: The member ports which are in this status can participate in user service traffic forwarding. The member ports in this status are called "the selected ports".
- Unselected: The member ports which are in this status cannot participate in user service traffic forwarding. The member ports in this status are called "the unselected ports".

The rate and duplex mode of an aggregation group is determined by the selected ports in the aggregation group. The rate of an aggregation group is the sum of all selected ports, and the duplex mode of the aggregation group is the same as the duplex mode of the selected ports.

Operation Key

An operation key is the property configuration of member ports. It consists of the rate, duplex mode, and administrative key (that is, the aggregation group number). In property configuration, change of the duplex mode or rate may cause re-calculation of the operation key.

In one aggregation group, if the duplex modes or rates of member ports are different, then the generated operation keys are different. However, the member ports that are in the selected status must have the same operation key.

LACP

Link Aggregation Control Protocol (LACP) is a protocol that is based on IEEE802.3ad. In LACP, Link Aggregation Control Protocol Data Units (LACP PDU) are used to interchange messages between two ends.

LACP Priorities

LACP priorities are categorized into two types: system LACP priorities and port LACP priorities.

- System LACP priorities: They are used to determine the LACP priority order of the devices at two ends.

- Port LACP priorities: They are used to determine the priority order at which the member ports of the local device are selected.

System ID and Port ID

System ID: Aggregation property of a device. It consists of the system LACP priority of the device and the system MAC address. The higher the system LACP priority is, the better the system ID of the device is. If the system LACP priorities are the same, then the smaller the system MAC address is, the better the system ID of the device is.

Port ID: Aggregation property of a port. It consists of the port LACP priority and the port number. The higher the port LACP priority is, the better the port ID is. If the port LACP priorities are the same, then the smaller the port number is, the better the port ID is.

Root Port of an Aggregation Group

The protocols that are applied in an aggregation group receive and send protocol packets through the root port of the aggregation group. The root port of an aggregation group is selected from the member ports of the aggregation group. The physical link of the root port must be in the up status.

21.1.2 Link Aggregation Modes *-B -S -E -A*

Link aggregation modes include the static aggregation mode and the dynamic aggregation mode. Aggregation groups are categorized into static aggregation groups and dynamic aggregation groups.

Static Aggregation Mode

In static aggregation mode, the LACP protocol of the member ports of the devices at the two ends is in the disabled status. In the static aggregation group of the local device, set the selected and unselected status for the member ports by following the guidelines as described below:

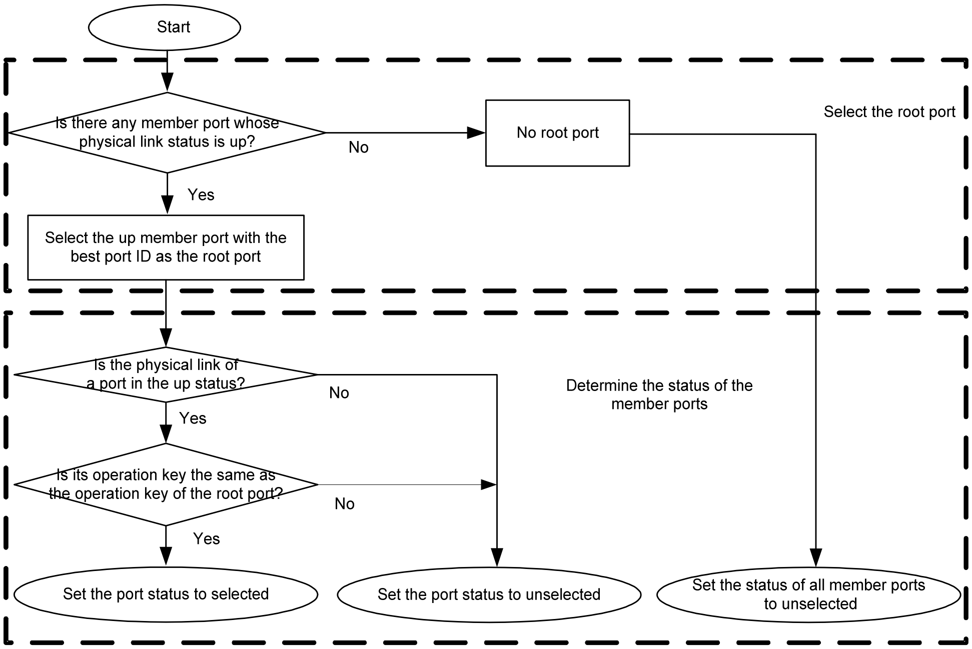

Start
Select the root port
Is there any member port whose physical link status is up?
No
No root port
Yes
Select the up member port with the best port ID as the root port
Is the physical link of a port in the up status?
No
Determine the status of the member ports
Yes
Is its operation key the same as the operation key of the root port?
No
Yes
Set the port status to selected
Set the port status to unselected
Set the status of all member ports to unselected

Figure 21-1 Setting the Status of Member Ports in Static Aggregation Mode

Dynamic Aggregation Mode

In dynamic aggregation ports, a port can join in a dynamic aggregation group in two modes, active or passive.

- If the duplex mode of the port is full duplex:

If the port joins in a dynamic aggregation group in active mode, the LACP protocol is enabled for the port.

If the port joins in a dynamic aggregation group in passive mode, the LACP protocol is disabled for the port. After it receives the LACP PDU packets from the peer port, the LACP protocol is enabled.

- If the duplex mode of the port is half duplex, no matter the port joins in a dynamic aggregation group in either mode, the LACP protocol is disabled for the port.

In the dynamic aggregation group, set the selected and unselected status for the member ports by following the guidelines as described below:

First determine the device with a better system ID. Then the device determines the statuses of the member ports of the devices at the two ends. The device with the better system ID sets the selected and unselected status for the member ports by following the guidelines as described below:

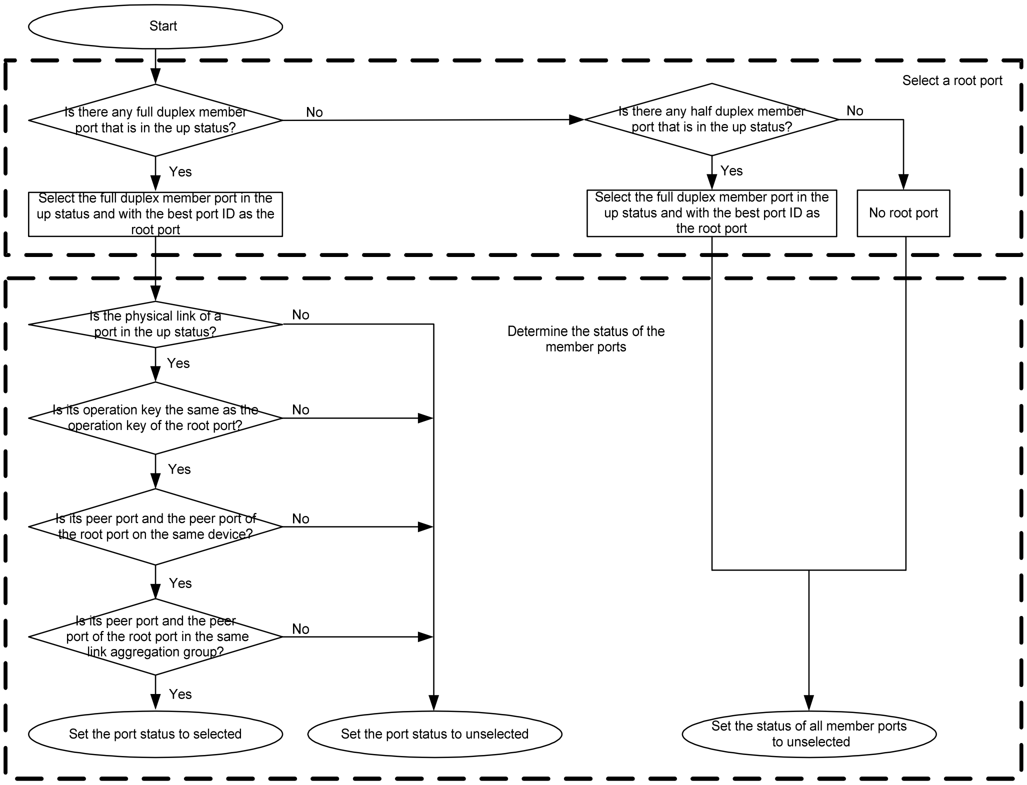

Start
Select a root port
Is there any full duplex member port that is in the up status?
No
Is there any half duplex member port that is in the up status?
No
Yes
Yes
Select the full duplex member port in the up status and with the best port ID as the root port
Select the full duplex member port in the up status and with the best port ID as the root port
No root port
Is the physical link of a port in the up status?
No
Determine the status of the member ports
Yes
Is its operation key the same as the operation key of the root port?
No
Yes
Is its peer port and the peer port of the root port on the same device?
No
Yes
Is its peer port and the peer port of the root port in the same link aggregation group?
No
Yes
Set the port status to selected
Set the port status to unselected
Set the status of all member ports to unselected

Figure 21-2 Setting the Status of Member Ports in Dynamic Aggregation Mode

21.2 Load-Balance Template Overview

1.2.1 Load-Balance *-B -S -E -A*

Load-Balance: When the outlet of network traffic is aggregation group, the chip may, depending on the current HASH configuration condition, implement the load balance of traffic among the member ports of the aggregation group, in order to increase the aggregate group's bandwidth utilization coefficient.

1.2.2 HASH KEY *-B -S -E -A*

HASH KEY: When selecting the specific outlet ports of aggregation group for network traffic, the chip performs HASH calculation to determine the KEY value for the outlet ports. Generally speaking, the HSAH KEY supported by different message types varies and the HASH KEY value supported by different switch chips also varies. The HASH KEYs supported by different messages are as shown in Table 1-1.

Table 21-1 HASH KEY Values Supported by Different Message Types and Their Meanings

HASH KEY type	Description
dst-mac	Load balancing based on the destination MAC addresses: The aggregation group implements aggregated load balancing based on the destination MAC addresses of messages.
src-mac	Load balancing based on the source MAC addresses: The aggregation group implements aggregated load balancing based on the source MAC addresses of messages.
src-interface	Load balancing based on the receiver source interface: The aggregation group implements aggregated load balancing based on the receiver source interface of messages.
vlan	Load balancing based on VLAN: The aggregation group implements aggregated load balancing based on the VLAN of messages.
dst-ip	Load balancing based on the destination IP addresses: The aggregation group implements aggregated load balancing based on the destination IP addresses of messages.

HASH KEY type	Description
l4-dst-port	Load balancing based on L4 destination port: The aggregation group implements aggregated load balancing based on the L4 destination port of messages.
flow-label	Load balancing based on IPv6 traffic tag: The aggregation group implements aggregated load balancing based on the IPv6 traffic tag of messages.
protocol	Load balancing based on IP protocol: The aggregation group implements aggregated load balancing based on the IP protocol of messages.
src-ip	Load balancing based on the source IP addresses: The aggregation group implements aggregated load balancing based on the source IP addresses of messages.
l4-src-port	Load balancing based on L4 source port: The aggregation group implements aggregated load balancing based on the L4 source port of messages.

In this Device, the HASH KEYs supported by different messages are as shown in Table 1-2.

Table 21-2 HASH KEYs Supported by Different Messages

Message type	Supported HASH KEYs
L2 known unicast messages	dst-mac, src-mac, src-interface, vlan
L3 known unicast messages	dst-ip, l4-dst-port, dst-mac, flow-label, protocol, src-ip, l4-src-port, src-mac, src-interface, vlan
Other L2 messages	dst-mac, src-mac, src-interface
Other L3 (IPv4/IPv6) messages	dst-ip, src-ip, src-interface

NOTE

- L2 known unicast messages' HASH KEY may support one or more HASH KEY combinations.

- L3 known unicast messages' HASH KEY may support one or more HASH KEY combinations.
- Other L2 messages' HASH KEY is fixed and nonconfigurable and invariably uses dst-mac, src-mac, src-interface for load balancing.
- Other L3 (IPv4/IPv6) messages' HASH KEY is fixed and nonconfigurable and invariably uses dst-ip, src-ip, src-interface for load balancing.

1.2.3 Load-Balance Template *-B -S -E -A*

Load-Balance template is a user-template concept specifically introduced to shield the chip difference between difference chip manufacturers. User refers to all businesses (i.e., business modules, such as LAC) that require the use of chip load balancing; template refers to a reusable HASH configuration scheme abstracted from bottom HASH resources.

Load-Balance templates can be distinguished by template name, which has a length no more than 31 characters. By default, the system will have a default HASH template named default. In addition to the default template, the user may also be provided customizable templates depending on current operation mode (standalone/stacking mode) and available chip resources. Each template is generally formed by the combination of L2 messages HASH KEY configurations and L3 message HASH KEY configurations.

The user may, depending on actual needs, flexibly configure Load-Balance template and corresponding template's HASH KEY. Upon completion of the configuration, the user may refer to or bind the corresponding template to implement load balance of traffic in accordance with corresponding template configuration.

NOTE

- Load-Balance template's name shall not be longer than 31 characters.
- The default Load-Balance template's name default cannot be changed.
- The Load-Balance template default cannot be deleted but can be configured.

21.3 Configuration of Load-Balance Template's Functions

Table 21-3 Functional Configuration List of Load-Balance Template

Configuration task	
Load-Balance template configuration function	Create a Load-Balance template, and enter the template configuration mode
	Configure Load-Balance template's HASH KEY

Configuration task	
	Delete Load-Balance template

21.3.1 Create Load-Balance Template *-B -S -E -A*

Once the Load-Balance template is successfully created, the system will enter corresponding Load-Balance template configuration mode.

NOTE

- In standalone mode, up to 1 user custom template can be created.
- In stacking mode, the creation of user custom template is not supported.

Configuration Conditions

None

Create Load-Balance Template

Table 21-4 Create Load-Balance Template

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create Load-Balance template	**load-balance profile** { *profile-name* | default }	Required

NOTE

- By default, the system has created a default template, and the user can access the default template configuration mode directly with the create command.
- The created template name only supports English and shall not be longer than 31 characters.

21.3.2 Configure Load-Balance Template's HASH KEY *-B -S -E -A*

Once the Load-Balance template is created and the template configuration mode is accessed, the user can configure the corresponding Load-Balance template's HASH KEY value.

NOTE

- By default, the default template created by the system will configure a set of default

HASH KEYs, the user may also modify the configuration depending on actual needs.

- The “default” template's default configuration is: L2:src-mac, dst-mac; Ip:src-ip, dst-ip.

NOTE

- Once a user custom template is created, by default the new template has not be configured any HASH KEY value, the user has to properly configure the HASH KEY for business binding.

Configuration Conditions

None

Configure Load-Balance Template's HASH KEY

Table 21-5 HASH KEY Configure Load-Balance Template's HASH KEY

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter Load-Balance template configuration mode	**load-balance profile** { *profile-name* | default }	Required Similar to the command Create Load-Balance template
Configure HASH KEY for L2 known unicast message load	**l2** { [**dst-mac**] [**src-mac**] [**src-interface**] [**vlan**] }	Required Can be the combination of one or more HASH KEYs
Configure HASH KEY for L3 known unicast message load	**ip** { [**dst-ip**] [**l4-src-port**] [**l4-dst-port**] [**protocol**] [**src-interface**] [**src-ip**] [**src-mac**] [**vlan**] [**dst-mac**] [**flow-label**] }	Required Can be the combination of one or more HASH KEYs
Activate current HASH KEY configuration	**active configuration pending**	Required
Cancel current HASH KEY configuration	**abort configuration pending**	Required

NOTE

- The HASH KEY value configured with l2 or ip command is in pending state and will not take effect immediately. It has to be activated with active configuration pending in order to take effect.
- The HASH KEY value configured with l2 or ip command is in pending state and will not take effect immediately. The user can use abort configuration pending command to cancel current configuration.
- During the configuration of new HASH KEY, the original HASH KEY will not be overwritten. The activation of the new HASH KEY with active command will result in the merge of the HASH KEY and the newly configured HASH KEY into a combination.
- The cancellation of the currently pending HASH KEY with the abort command will not change the original HASH KEY.
- If the activation fails, the pending HASH KEY will not be erased. Generally activation failures are caused by improperly configured HASH KEY.
- User custom Load-Balance template can be used to configure any HASH KEY. However, when the template is used for business binding, it is required that the bound template's L2 and L3 have at least one valid HASH KEY.
- Requirement for “default”template: L2 and L3 HASH KEY shall be configured at least one HASH KEY.

21.3.3 Delete Load-Balance Template *-B -S -E -A*

Delete Load-Balance Template

NOTE

- By default, the default template created by the system is not deletable.
- When a business referenced or bound template is not deletable, all reference/binding relations has to be removed before the template can be deleted.
- Nonexistent templates cannot be deleted.

Configuration Conditions

None

Delete Load-Balance Template

Table 21-6 Delete Load-Balance Template

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter Load-Balance template configuration mode	**no load-balance profile** { *profile-name* }	Required

21.4 Link Aggregation Function Configuration

Table 21-7 Link Aggregation Function List

Configuration Tasks	
Configure an aggregation group.	Create an aggregation group.
	Add ports into the aggregation group.
Configure the load balancing mode of the aggregation group.	Configure the load balancing mode of the aggregation group.
Configure LACP priorities.	Configure the system LACP priority.
	Configure the port LACP priority.

21.4.1 Configure an Aggregation Group *-B -S -E -A*

After configuring an aggregation group, you can manage multiple physical ports in a centralized manner. Any configuration on the aggregation group will be applied to each member port.

NOTE

- A device supports a maximum of 32 aggregation groups, a maximum of 8 ports can join in the aggregation group at the same time, and a maximum of 8 ports can be in the selected status at the same time.

Configuration Conditions

None

Create an Aggregation Group

The aggregation groups at the two ends of an aggregated link must be configured to the same type. Description can be added to each aggregation group to make it easier for network administrators to distinguish the aggregation groups.

Table 21-8 Creating an Aggregation Group

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Create an aggregation group.	**link-aggregation** *link-aggregation-id* **mode** { **manual** | **lacp** }	Mandatory. By default, no aggregation group is created.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	-
Configure the description for the aggregation group.	**description** *description-name*	Optional. By default, no description is added to the aggregation group.

NOTE

- The protocols that are applied in an aggregation group receive and send protocol packets through the root port of the aggregation group. In static aggregation mode, because the member ports between the devices at two ends do not exchange LACP PDU packets, the root ports of the two devices may be on different physical links. In this way, other protocol packets on the aggregation group may fail to be received or sent. To prevent this problem, ensure that the root ports of the devices at the two ends are on the same physical link. In dynamic aggregation mode, the member ports of the devices at two ends exchange LACP PDU packets. The negotiation between the two member ports ensures that the root ports of the two devices are on the same physical link.
- After an aggregation group is deleted, all the member ports of the aggregation group are removed from the aggregation group, and then the all the member ports adopt the default settings. This may result in loops in the network. Therefore, before deleting an aggregation group, ensure that the STP function has been enabled or ensure that no loop may occur in the network.

Add Ports into the Aggregation Group

When an aggregation group is created, it is only a logic interface which contains no physical port. In this case, the aggregation function does not take effect. The aggregation function takes effect after ports are added to a static aggregation group. The aggregation function takes effect after local or peer ports are added into a dynamic aggregation group.

Table 21-9 Adding a Port into the Aggregation Group

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Add the port into the aggregation group.	**link-aggregation** *link-aggregation-id* { **manual | active | passive** }	By default, a port is not added into any aggregation group.

NOTE

- Before adding a port into an aggregation group, the aggregation group must have been created; otherwise, an error message is displayed.
- A port can be added one aggregation group at a time.
- After a port is added into an aggregation group, the some existing configurations (such as loopback detection and VLAN) will be removed from the port.
- Some functions (such as loopback detection) cannot be configured on a member port in an aggregation group; otherwise, an error message is displayed.
- If a port is added into a dynamic aggregation group in passive mode, its peer port must be added into the dynamic aggregation group in active mode. Otherwise, the two ports are both in the unselected status and they cannot participate in user service traffic forwarding.

21.4.2 Configure the Load Balancing Mode of an Aggregation Group

-B -S -E -A

By configuring the load balancing mode of an aggregation group, you can achieve load balancing of service traffic in the aggregation group in a flexible manner.

Configuration Conditions

None

Configure the Load Balancing Mode of the Aggregation Group

Table 21-10 Configuring the Load Balancing Mode of the Aggregation Group

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-

Step	Command	Description
Configure the load balancing mode of the aggregation group.	**link-aggregation** *link-aggregation-id* **load-balance** { **dst-ip** | **dst-mac** | **enh-hash** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac** }	Mandatory. By default, the aggregation group implements aggregated load balancing based on the source MAC addresses of packets.
Configure the load balancing mode of the aggregation group to the enhanced mode.	**link-aggregation load-balance enhanced-hash mode** { **ip** | **mac** }	Optional. In configuring the load balancing mode of the aggregation group, the **enh-hash** option is selected, and the configuration takes effect. By default, in the enhanced mode, the aggregation group implements aggregated load balancing based on the source or destination MAC addresses of packets.

21.4.3 Configure LACP Priorities *-B -S -E -A*

Configuration Conditions

None

Configure the System LACP Priority

Configuration of the system LACP priority may affect the system ID, and finally affect the selected/unselected status of member ports of dynamic aggregation groups.

Table 21-11 Configuring the System LACP Priority

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Configure the system LACP priority.	**lacp system-priority** *system-priority-value*	Mandatory.

Step	Command	Description
		By default, the system LACP priority is 32768.

Configure the Port LACP Priority

Configuration of the port LACP priority may affect the port ID, and finally affect the selected/unselected status of member ports of aggregation groups.

Table 21-12 Configuring the Port LACP Priority

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	-
Configure the port LACP priority.	**lacp port-priority** *port-priority-value*	Mandatory. By default, the port LACP priority is 32768.

21.4.4 Configure Hot Swap Fast Switching Root Port *-B -S -E -A*

If the hot swap fast switching root port is properly configured, when the card on which the root port is located is hot swapped in/pulled out, the system will immediately notify the opposite port to reselect a root port to facilitate the fast stabilization and convergence of the aggregation group.

NOTE

- The system will send fast switching notification only after the card on which the root port is located has been pulled out.
- Static aggregation group will not send fast switching notifications.

Configuration Conditions

None

Configure Hot Plug Fast Switching Root Port

Table 21-13 Configure Hot Plug Fast Switching Root Port

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure hot swap fast switching root port	**link-aggregation hotswap fast-change-rootport**	Required By default, hot swap fast switching root port is not configured

21.4.5 Link Aggregation Monitoring and Maintaining *-B -S -E -A*

Table 21-14 Link Aggregation Monitoring and Maintaining

Command	**Description**
show link-aggregation group [*link-aggregation-id*]	Displays brief information about a specified aggregation group or all existing aggregation groups.
show link-aggregation interface [*interface-name*]	Displays the details of a specified member port of an aggregation group or details of all member ports of the aggregation group.

21.5 Typical Configuration Example of Link Aggregation

21.5.1 Configure a Static Aggregation Group *-B -S -E -A*

Network Requirements

- Device1 is connected to PC1, Device2 is connected to PC2 and PC3, and the three PCs are in the same network segment. Device1 and Device2 are interconnected through Trunk ports.
- A static aggregation group is configured between Device1 and Device2 for bandwidth increase, load sharing, and service backup.

Network Topology

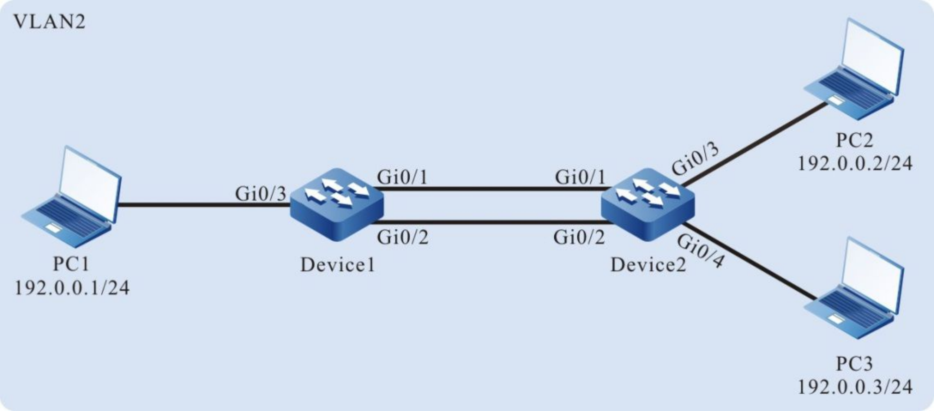


Figure 21-3 Networking for Configuring a Static Aggregation Group

Configuration Steps

Step 1: Create a static aggregation group.

#On Device1, create static aggregation group 1.

```
Device1#configure terminal
Device1(config)#link-aggregation 1 mode manual
```

#On Device2, create static aggregation group 2.

```
Device2#configure terminal
Device2(config)#link-aggregation 1 mode manual
```

Step 2: Add ports into the aggregation group.

#On Device1, add ports gigabitethernet0/1 and gigabitethernet0/2 into aggregation group 1 in Manual mode.

```
Device1(config)#interface gigabitethernet 0/1,0/2
Device1(config-if-range)#link-aggregation 1 mode manual
Device1(config-if-range)#exit
```

#On Device2, add ports gigabitethernet0/1 and gigabitethernet0/2 into aggregation group 1 in Manual mode.

```
Device2(config)#interface gigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 mode manual
Device2(config-if-range)#exit
```

#After the configuration is completed, check the status of aggregation group 1 on the devices.

Here takes Device1 for example:

```
Device1#show link-aggregation group 1
 Link Aggregation 1
  Mode: Manual   Description:
  Load balance method: dst-ip
  Number of ports in total: 2
  Number of ports attached: 2
  Root port: gigabitethernet0/1
  gigabitethernet0/1: ATTACHED
  gigabitethernet0/2: ATTACHED
```

According to the system display, ports gigabitethernet0/1 and gigabitethernet0/2 are both in the ATTACHED state in aggregation group 1, and aggregation of aggregation group 1 is successful.

NOTE

- For the method of checking Device2, refer to the method of checking Device1.

Step 3: Configure the load balancing mode of the aggregation group.

#On Device1, configure the load balancing mode of aggregation group 1 to the dst-ip mode.

```
Device1(config)#link-aggregation 1 load-balance dst-ip
```

Step 4: Configure a VLAN, and configure the link type of the aggregation group and ports.

#On Device1, create VLAN2, configure the link type of aggregation group 1 to Trunk and allow services of VLAN2 to pass, and set Port VLAN ID (PVID) to 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#exit
Device1(config)#link-aggregation 1
Device1(config-link-aggregation1)#switchport mode trunk
Device1(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device1(config-link-aggregation1)#switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
```

#On Device1, configure the link type of port gigabitethernet0/3 to Access and allow services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode access
Device1(config-if-gigabitethernet0/3)#switchport access vlan 2
Device1(config-if-gigabitethernet0/3)#exit
```

#On Device2, create VLAN2, configure the link type of aggregation group 1 to Trunk and allow services of VLAN2 to pass, and set PVID to 2. (Omitted)

#On Device2, configure the link type of ports gigabitethernet0/3 and gigabitethernet0/4 to Access and allow services of VLAN2 to pass. (Omitted)

Step 5: Check the result.

#On the devices, check the aggregated bandwidth of aggregation group 1.

Here takes Device1 for example:

```
Device1#show link-aggregation 1
link-aggregation 1 configuration information
    Description     :
    Status          : Enabled
    Link            : Up
    Act Speed       : 2000
    Act Duplex      : Full
    Port Type       : Nni
```

```
                Pvid              : 2
```

According to the system display, the interface bandwidth of aggregation group 1 on Device1 is 2000 M.

NOTE

- For the method of checking Device2, refer to the method of checking Device1.

#On Device1, check the current load balancing mode of aggregation group1.

```
Device1#show link-aggregation group 1
 Link Aggregation 1
  Mode: Manual   Description:
  Load balance method: dst-ip
  Number of ports in total: 2
  Number of ports attached: 2
  Root port: gigabitethernet0/1
  gigabitethernet0/1: ATTACHED
  gigabitethernet0/2: ATTACHED
```

According to the system display, the current load balancing mode of aggregation group 1 is dst-ip.

#During the process of service interaction between PC1 and PC2 and PC3, load balancing of data is achieved on the aggregated links. If a link in the aggregation group becomes faulty, the other links provide service backup.

21.5.2 Configure a Dynamic Aggregation Group *-B -S -E -A*

Network Requirements

- Device1 is connected to PC1, Device2 is connected to PC2 and PC3, and the three PCs are in the same network segment. Device1 and Device2 are interconnected through Trunk ports.
- A dynamic aggregation group is configured between Device1 and Device2 for bandwidth increase, load sharing, and service backup.

Network Topology

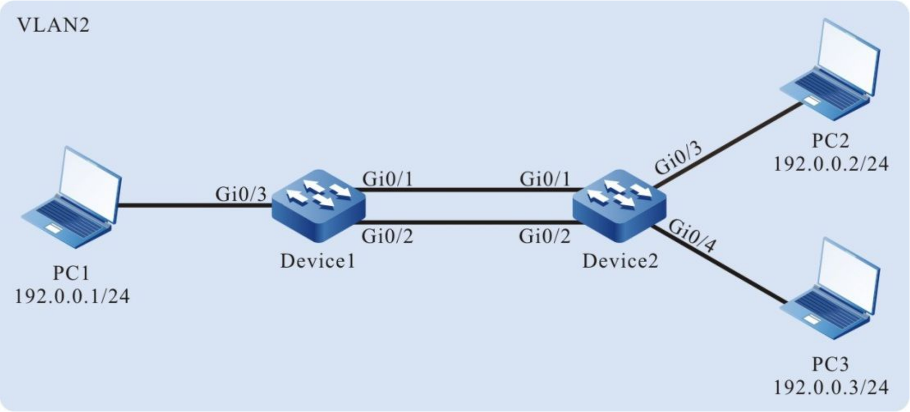


Figure 21-4 Networking for Configuring a Dynamic Aggregation Group

Configuration Steps

Step 1: Create a dynamic aggregation group.

#On Device1, create dynamic aggregation group 1.

```
Device1#configure terminal
Device1(config)#link-aggregation 1 mode lacp
```

#On Device2, create dynamic aggregation group 1.

```
Device2#configure terminal
Device2(config)#link-aggregation 1 mode lacp
```

Step 2: Add ports into the aggregation group.

#On Device1, add ports gigabitethernet0/1 and gigabitethernet0/2 into aggregation group 1 in Active mode.

```
Device1(config)#interface gigabitethernet 0/1,0/2
Device1(config-if-range)#link-aggregation 1 mode active
Device1(config-if-range)#exit
```

#On Device2, add ports gigabitethernet0/1 and gigabitethernet0/2 into aggregation group 1 in Active mode.

```
Device2(config)#interface gigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 mode active
Device2(config-if-range)#exit
```

#After the configuration is completed, check the status of aggregation group 1 on the devices.

Here takes Device1 for example:

```
Device1#show link-aggregation group 1
 Link Aggregation 1
  Mode: LACP   Description:
  Load balance method: dst-ip
  Number of ports in total: 2
  Number of ports attached: 2
  Root port: gigabitethernet0/1
  gigabitethernet0/1: ATTACHED
  gigabitethernet0/2: ATTACHED
```

According to the system display, ports gigabitethernet0/1 and gigabitethernet0/2 are both in the ATTACHED state in aggregation group 1, and aggregation of aggregation group 1 is successful.

NOTE

- For the method of checking Device2, refer to the method of checking Device1.

Step 3: Configure the load balancing mode of the aggregation group.

#On Device1, configure the load balancing mode of aggregation group 1 to the dst-ip mode.

```
Device1(config)#link-aggregation 1 load-balance dst-ip
```

Step 4: Configure a VLAN, and configure the link type of the aggregation group and ports.

#On Device1, create VLAN2, configure the link type of aggregation group 1 to Trunk and allow services of VLAN2 to pass, and set PVID to 2.

```
Device1(config)#vlan 2
Device1(config-vlan2)#exit
Device1(config)#link-aggregation 1
Device1(config-link-aggregation1)#switchport mode trunk
Device1(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device1(config-link-aggregation1)#switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
```

#On Device1, configure the link type of port gigabitethernet0/3 to Access and allow services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode access
Device1(config-if-gigabitethernet0/3)#switchport access vlan 2
Device1(config-if-gigabitethernet0/3)#exit
```

#On Device2, create VLAN2, configure the link type of aggregation group 1 to Trunk and allow services of VLAN2 to pass, and set PVID to 2. (Omitted)

#On Device2, configure the link type of ports gigabitethernet0/3 and gigabitethernet0/4 to Access and allow the services of VLAN2 to pass. (Omitted)

Step 5: Check the result.

#On the devices, check the aggregated bandwidth of aggregation group 1.

Here takes Device1 for example:

```
Device1#show link-aggregation 1
link-aggregation 1 configuration information
    Description     :
    Status          : Enabled
    Link            : Up
    Act Speed       : 2000
    Act Duplex      : Full
    Port Type       : Nni
    Pvid            : 2
```

According to the system display, the interface bandwidth of the aggregation group on Device1 is 2000 M.

NOTE

- For the method of checking Device2, refer to the method of checking Device1.

#After the configuration is completed, check the current load balancing mode on Device1.

```
Device1#show link-aggregation group 1
 Link Aggregation 1
  Mode: LACP   Description:
  Load balance method: dst-ip
  Number of ports in total: 2
  Number of ports attached: 2
  Root port: gigabitethernet0/1
```

```
gigabitethernet0/1: ATTACHED
gigabitethernet0/2: ATTACHED
```

According to the system display, the current load balancing mode of aggregation group 1 is dst-ip.

#During the process of service interaction between PC1 and PC2 and PC3, load balancing of data is achieved on the aggregated links. If a link in the aggregation group becomes faulty, the other links provide service backup.

22 Port Isolation

22.1 Overview

Port isolation is a security feature that is based on ports. According to the actual requirement, you can configure certain ports to be isolated from a specified port, that is, configure some isolated ports for a specified port. In this way, the packets that are received by the specified port cannot be forwarded to the isolated ports. This enhances the network security, and also provides a flexible networking scheme.

22.2 Port Isolation Function Configuration

Table 22-1 Port Isolation Function List

Configuration Tasks	
Configure the basic function of port isolation.	Configure port isolation.
Configure the isolation function for member ports of the aggregation group.	Configure the isolation function for member ports of the aggregation group.

22.2.1 Configure Basic Functions of Port Isolation *-B -S -E -A*

The port isolation function realizes unidirectional packet isolation. Assuming that port B is configured as the isolated port of port A, then if a packet whose target port is port B enters port A, the port is directly discarded. However, if a packet whose target port is port B enters port B, the port is normally forwarded. The isolated port can be a port or an aggregation group.

Configuration Conditions

None

Configure Port Isolation

Table 22-2 Configuring Port Isolation

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the global configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configuring isolated ports.	**isolate-port** { **interface** *interface-list* **| link-aggregation** *link-aggregation-id* }	Mandatory. By default, no isolated port is configured.

NOTE

- In configuring isolated ports, ensure that the isolated ports have not been added into any aggregation group; otherwise, the isolation operation fails.
- To isolate an aggregation group, ensure that the aggregation group exists; otherwise, the isolation operation fails.

22.2.2 Configure the Isolation Function for Member Ports of an Aggregation Group

-B -S -E -A

Through port isolation, member ports of an aggregation group can be isolated. In this way, the packets received by a member port of the aggregation group will not be forwarded to the other member ports of the aggregation group.

Configuration Conditions

None

Configure the Isolation Function for Member Ports of the Aggregation Group

Table 22-3 Configuring the Isolation Function for Member Ports of the Aggregation Group

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	-
Enable the member port isolation function in the aggregation group.	**link-aggregation member-isolate**	Mandatory. By default, the member port isolation function is disabled for an aggregation group.

NOTE

- Usually, the packets received by a member port of an aggregation group will not be forwarded to other member port of the aggregation group. However, in the VLAN N:1 environment, this feature of the aggregation group is not supported. In this way, the member port isolation function is used to provide the feature in the aggregation group.

22.2.3 Port Isolation Monitoring and Maintaining *-B -S -E -A*

Table 22-4 Port Isolation Monitoring and Maintenance

Command	Description
show isolate-port	Displays the configuration of port isolation.

22.3 Typical Configuration Example of Port Isolation

22.3.1 Configure Port Isolation *-B -S -E -A*

Network Requirements

- PC1 and PC2 are connected to Device, and they are in the same VLAN, VLAN2.
- On Device, port isolation has been configured; therefore, PC1 and PC2 cannot communicate with each other.

Network Topology

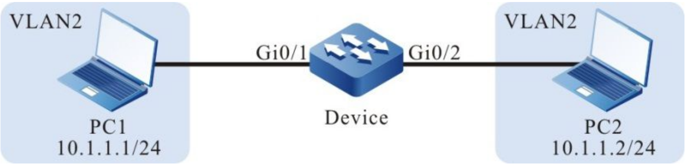


Figure 22-1 Networking for Configuring Port Isolation

Configuration Steps

Step 1: Configure a VLAN, and configure the link type of the ports.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Access and allow the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure port isolation.

#On Device, configure port isolation between port gigabitethernet0/1 and port gigabitethernet0/2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#isolate-port interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/1)#exit
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#isolate-port interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/2)#exit
```

#On Device, query the port isolation information.

```
Device#show isolate-port
------------------------------------------------------------------------
Interface        :gigabitethernet0/1
Isolated Interface:gi0/2
------------------------------------------------------------------------
Interface        :gigabitethernet0/2
Isolated Interface:gi0/1
```

Step 3: Check the result.

#PC1 and PC2 cannot communicate with each other.

23 VLAN

23.1 Overview

In a switched Ethernet, each port in the device is an independent collision domain, but all the ports belong to a broadcast domain. When a terminal device sends broadcast packets, all devices in the LAN can receive the packets. This not only wastes network bandwidth, but also brings hidden troubles.

Virtual VLAN is a technology through which devices in the same LAN can be divided in a logic manner. The devices in the same VLAN can communicate with each other at layer 2, while the devices from different VLANs are isolated at layer 2. In this way, broadcast packets are limited within a VLAN.

VLANs comply with IEEE 802.1Q. This standard defines a new frame encapsulation format, in which a 4-byte VLAN tag containing VLAN information is added after the source MAC address of a traditional data frame.

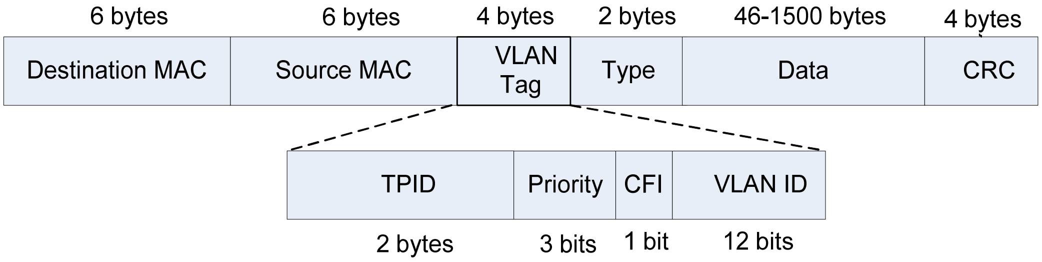


Figure 23-1 IEEE 802.1Q Frame Encapsulation Format

A VLAN tag contains the following four fields:

- Tag Protocol Identifier (TPID): It is used to determine whether a VLAN tag is carried by the data frame. The length is 2 bytes, and the value is fixed to be 0x8100, indicating a standard 802.1Q tag.
- Priority: It is the 802.1p priority. The length is 3 bits and the value range is 0-7. Packets with different priorities can obtain services of different levels.
- Canonical Format Indicator (CFI): It indicates whether the MAC address is encapsulated in a standard format for transmission in different media. The length is 1 bit. The value 0 indicates that the MAC address is encapsulated in a standard format while the value 1 indicates that the MAC address is encapsulated in a non-standard format.
- VLAN ID: It indicates the VLAN to which the packet belongs. The length is 12 bits, and the value range is 0-4095, where 0 and 4095 are protocol reserved values, and the available VLAN IDs are in the range of 1-4094.

VLANs have the following advantages:

- Establishes virtual workgroups flexibly. Users with the same requirements can be divided into one VLAN, without being limited by their physical locations.
- Limits broadcast domains. A VLAN is a broadcast domain. Layer-2 unicast, multicast, and broadcast frames can be forwarded only within the domain, and they cannot enter

other VLANs directly. This prevents broadcast storms.

- Improves the network security. Different VLANs are isolated at layer two, and the VLANs cannot communicate with each other directly.

According to applications, VLANs are categorized into the following four types:

- Port-based VLANs
- MAC address-based VLANs
- IP subnet-based VLANs
- Protocol-based VLANs

By default, in the order of priorities from high to low, the four types of VLANs are: MAC address-based VLANs, IP subnet-based VLANs, protocol-based VLANs, and port-based VLANs. On one port, the VLAN takes effect according to the priority levels, and only one type of VLAN takes effect.

23.2 VLAN Function Configuration

Table 23-1 VLAN Function List

Configuration Tasks	
Configuring basic attributes of VLANs	Configure a VLAN.
	Configure the VLAN name.
Configure a port-based VLAN.	Configure the port link type.
	Add an Access port into the VLAN.
	Configure a Trunk port to allow services of a VLAN to pass.
	Add a Hybrid port into the VLAN.
	Configure PVIDs for ports.
Configure a MAC address-based VLAN.	Configure a MAC address-based VLAN.
Configure an IP subnet-based VLAN.	Configure an IP subnet-based VLAN.
Configure a protocol-based VLAN.	Configure a protocol-based VLAN.
Configure the types of frames that can be received by the port.	Configure the types of frames that can be received by the port.

23.2.1 Configure Basic Attributes of VLANs *-B -S -E -A*

Configuration Conditions

None

Configure a VLAN

Each VLAN corresponds to a broadcast domain. The users in the same VLAN can communicate with each other at layer 2, while users from different VLANs are isolated from each other at layer 2.

Table 23-2 Configuring a VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create a VLAN.	**vlan** *vlan-list*	Mandatory. By default, the system automatically creates VLAN1. In creating a single VLAN, after a VLAN is created, you will enter the VLAN configuration mode. In creating multiple VLANs, after a VLAN is created, you are still in the current configuration mode.

Configure the VLAN Name

To facilitate memory and management, you can configure the name of a VLAN according to the service type, function, and connection of the VLAN.

Table 23-3 Configure the VLAN Name

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enters the VLAN configuration mode.	**vlan** *vlan-id*	-

Step	Command	Description
Configure the VLAN name.	**name** *vlan-name*	Mandatory. By default, the name of VLAN1 is DEFAULT, and the names of other VLANs follow the format "VLAN*vlan-id*", such as VLAN100.

23.2.2 Configure Port-Based VLANs *-B -S -E -A*

A port-based VLAN, also called port VLAN, is a VLAN of the simplest division type. After a port is added into the VLAN, the port can forward packets that belong to the VLAN.

Configuration Conditions

None

Configure the Port Link Type

A port handles VLAN tags in different modes before it forwards packets. According to the VLAN tag handling modes, the following three link types are available:

- Access type: The packets that have been forwarded do not carry VLAN tags. Ports of this type are usually connected to user devices.
- Trunk type: The packets from the VLANs in which the PVID is located do not carry VLAN tags, while the packets from other VLANs still carry VLAN tags.
- Hybrid type: The packets from the specified VLAN can be configured not to carry or carry VLAN tags. Ports of the type can be connected to user devices or interconnected with network devices.

The ports of the Trunk type and the ports of the Hybrid type cannot be converted to each other directly. They need to be converted to the Access type before being converted to another type.

Table 23-4 Configuring the Port Link Type

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the port link type.	**switchport mode** { **access** | **hybrid** | **trunk** }	Mandatory. By default, the port link type is the Access type.

NOTE

- Some commands can be configured only on the ports with the specified link type. Therefore, if the port link type is converted to another type, the functions that are configured on the port with the original link type may become invalid.

Add an Access Port into the VLAN

One Access port can belong to only one VLAN. When an Access port is added into a specified VLAN, it exits from the current VLAN and then enters the specified VLAN. If the VLAN to which the Access port is to be added does not exists, the VLAN is automatically created.

Table 23-5 Adding an Access Port into the VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		only within the aggregation group.
Configure the port link type to the Access type.	**switchport mode access**	Mandatory. By default, the port link type is the Access type.
Add an Access port into the specified VLAN.	**switchport access vlan** *vlan-id*	Mandatory. By default, the Access port is added into VLAN1.

Configure a Trunk Port to Allow Services of a VLAN to Pass

If a Trunk port allows services of an existing VLAN to pass, the port allows forwarding packets of the VLAN. If the VLAN that the Trunk port allows to pass does not exist, the VLAN will not be created automatically and you must create the VLAN before the port allows forwarding packets of the VLAN.

Table 23-6 Configuring a Trunk Port to Allow Services of a VLAN to Pass

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port link type to the Trunk type.	**switchport mode trunk**	Mandatory. By default, the port link type is the Access type.

Step	Command	Description
Configure a Trunk port to allow a VLAN to pass.	**switchport trunk allowed vlan** { **all** | **add** *vlan-list* }	Mandatory. By default, the Trunk port allows VLAN1 to pass.
Configure the packets from the VLAN in which the PVID is located to be forwarded with VLAN tags reserved.	**vlan dot1q tag pvid**	Optional. By default, the packets from the VLAN in which the PVID is located are forwarded without VLAN tags.

Add a Hybrid Port into the VLAN

If the VLAN to which the Access port is to be added does not exist, the VLAN is automatically created.

Table 23-7 Adding a Hybrid Port into the VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port link type to the Hybrid type.	**switchport mode hybrid**	Mandatory. By default, the port link type is the Access type.
Add a Hybrid port to a specified VLAN in a specified mode.	**switchport hybrid** { **untagged** | **tagged** } **vlan** *vlan-list*	Mandatory.

Step	Command	Description
		By default, the Hybrid port is added into VLAN1 in Untagged mode.

Configure PVIDs for Ports

Port VLAN ID (PVID) is an important parameter of a port. When a port receives an Untag packet, it adds a VLAN tag to the packet, and the VLAN ID of the VLAN tag is the PVID of the port.

The PVID of an Access port is the ID of the VLAN to which it belongs, so the PVID of the Access port can be configured only by changing the VLAN to which it belongs. The Trunk port and hybrid port can belong to multiple VLANs, and their PVIDs can be configured according to the actual requirement.

The Trunk port and Hybrid port must be added into the VLAN to which their PVIDs belong; otherwise, packets of the VLAN to which their PVIDs belong cannot be forwarded, and the port discards the received Untag packets.

Table 23-8 Configuring PVIDs for Ports

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configuring the PVID for the Trunk port.	**switchport trunk pvid vlan** *vlan-id*	Mandatory. Select one option according to the port link type. By default, the port PVID is VLAN1.
Configuring the PVID for the Hybrid port.	**switchport hybrid pvid vlan** *vlan-id*	

NOTE

- In configuring the PVID for a port, the VLAN to which the PVID belongs must have been created; otherwise, the configuration fails, and an error message is prompted.

23.2.3 Configure MAC Address-Based VLANs *-B -S -E -A*

MAC address-based VLANs, also called MAC VLANs, are classified according to the source MAC addresses of the packets. After a MAC VLAN is configured, if the port receives an Untag packet and the source MAC address of the packet matches a MAC VLAN entry, the system adds a VLAN tag for the packet, in which the VLAN ID matches the VLAN ID in the MAC VLAN entry.

After the physical location of the user is changed, if the MAC address of the user is not changed, the VLAN to which the user port belongs need not be re-configured. A device supports a maximum of 4096 MAC VLAN entries.

Configuration Conditions

None

Configure MAC Address-Based VLANs

Table 23-9 Configuring MAC Address-Based VLANs

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure a MAC VLAN entry.	**mac-vlan mac-address** *mac-address* **vlan** *vlan-id* [**pri** *priority*]	Mandatory. By default, no MAC VLAN entry is configured.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Enable the MAC VLAN function of the port.	**mac-vlan enable**	Mandatory. By default, the MAC VLAN function is disabled on the port.

NOTE

- The port on which the MAC VLAN function is enabled must be added into the VLAN that matches the entry; otherwise, the port cannot forward packets of the VLAN, and the packets that match the source MAC address will be discarded.

23.2.4 Configure IP Subnet-Based VLANs *-B -S -E -A*

IP subnet-based VLANs, also called IP subnet VLANs, are classified according to the source IP addresses of the packets. After an IP subnet VLAN is configured, if the port receives an Untag packet and the source IP address of the packet matches an IP subnet VLAN entry, the system adds a VLAN tag for the packet, in which the VLAN ID matches the VLAN ID in the IP subnet VLAN entry.

After the physical location of the user is changed, if the IP address of the user is not changed, the VLAN to which the user port belongs need not be re-configured. A device supports a maximum of 256 IP subnet VLAN entries.

Configuration Conditions

None

Configure IP Subnet-Based VLANs

Table 23-10 Configuring IP Subnet-Based VLANs

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure an IP subnet VLAN entry.	**ip-subnet-vlan ipv4** *ip-address* **mask** *mask* **vlan** *vlan-id* [**pri** *priority*]	Mandatory. By default, no IP subnet VLAN entry is configured.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected.

Step	Command	Description
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable the IP subnet VLAN function of the port.	**ip-subnet-vlan enable**	Mandatory. By default, the IP subnet VLAN function is disabled on the port.
Configure that the port matches IP subnet VLANs with priority, and then matches MAC VLANs.	**ip-subnet-vlan priority front**	Optional. By default, the port matches MAC VLANs with priority, and then matches IP subnet VLANs.

NOTE

- The port on which the IP subnet VLAN function is enabled must be added into the VLAN that matches the entry; otherwise, the port cannot forward packets of the VLAN, and the packets that match the source IP address will be discarded.

23.2.5 Configure Protocol-Based VLANs *-B -S -E -A*

Protocol-based VLANs, also called protocol VLANs, are classified according to the frame encapsulation formats and protocol types of packets. After a protocol profile is defined, a port is configured to match a protocol profile, and the protocol VLAN function is enabled for the port, if the port receives an Untag packet that matches the protocol profile, the port adds a VLAN tag for the packet. The VLAN ID matches the VLAN ID defined in the profile.

After the physical location of the user is changed, if the frame encapsulation format of the user packets and protocol type are not changed, the VLAN to which the user port belongs need not be re-configured. A device supports defining a maximum of 16 protocol profiles.

Configuration Conditions

None

Configure Protocol-Based VLANs

Table 23-11 Configuring Protocol-Based VLANs

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Define a protocol profile.	**protocol-vlan profile** *profile-index* **frame-type** *frame-type* **ether-type** *ether-type*	Mandatory. By default, no protocol profile is defined.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure a protocol that the port matches.	**protocol-vlan profile** *profile-index* **vlan** *vlan-id*	Mandatory. By default, the port does not match any protocol profile.
Enable the protocol VLAN function of the port.	**protocol-vlan enable**	Mandatory. By default, the protocol VLAN function is disabled on the port.

NOTE

- The port for which a matching protocol profile has been configured and the protocol VLAN function has been enabled must be added into the VLAN corresponding to the protocol profile that it matches; otherwise, the port cannot forward packets of the VLAN, and the packets matching the protocol will be discarded.

23.2.6 Configure the Types of Frames that Can Be Received by the Port

-B -S -E -A

Configuration Conditions

None

Configure the Types of Frames that Can Be Received by the Port

You can configure the types of frames that can be received by a port so that the port receives only Untag packets, receives only Tag packets, or receives both of them. The packets that fail to meet the requirement will be discarded.

Table 23-12 Configuring the Types of Frames that Can Be Received by the Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the types of frames that can be received by the port.	**switchport accept frame-type** { **all** | **untag** | **tag** }	Mandatory. By default, the type of frames that can be received by a port is all, that is, receiving both Untag and Tag packets.

23.2.7 VLAN Monitoring and Maintaining ***-B -S -E -A***

Table 23-13 VLAN Monitoring and Maintaining

Command	Description
show ip-subnet-vlan	Displays the information about IP subnet VLANs.
show mac-vlan	Displays the information about MAC VLANs.
show protocol-vlan [**profile**]	Displays the information about protocol VLANs.
show running-config vlan	Displays VLAN configuration information.
show vlan [*vlan-id*]	Displays the information about a specified VLAN or all existing VLANs.
show vlan statistics	Displays the number of existing VLANs.
show { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* } **vlan status**	Displays the VLAN information on the specified port or aggregation group.

23.3 VLAN Typical Configuration Example

23.3.1 Configure Port-Based VLANs

-B -S -E -A

Network Requirements

- Server1 and PC1 are in the office network, while Server2 and PC2 are in the production network.
- You need to configure the port-based VLAN functions to isolate PC1 and PC2 so that PC1 can access only Server1 and PC2 can access only Server2.

Network Topology

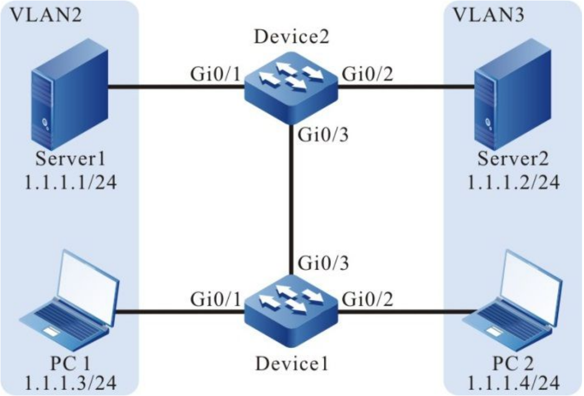


Figure 23-2 Networking for Configuring Port-Based VLANs

Configuration Steps

Step 1: On Device1, configure VLANs, and configure the port link types of the ports.

#On Device1, create VLAN2 and VLAN3.

```
Device1#configure terminal
Device1(config)#vlan 2-3
```

#On Device1, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Access. Configure gigabitethernet0/1 to allow services of VLAN2 to pass and configure gigabitethernet0/2 to allow services of VLAN3 to pass.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode access
Device1(config-if-gigabitethernet0/1)#switchport access vlan 2
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)#interface gigabitethernet0/2
Device1(config-if-gigabitethernet0/2)#switchport mode access
Device1(config-if-gigabitethernet0/2)#switchport access vlan 3
Device1(config-if-gigabitethernet0/2)#exit
```

#On Device1, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN2 and VLAN3 to pass.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode trunk
Device1(config-if-gigabitethernet0/3)#switchport arunk allowed vlan add 2-3
Device1(config-if-gigabitethernet0/3)#exit
```

Step 2: On Device3, configure VLANs, and configure the port link types of the ports.

#On Device2, create VLAN2 and VLAN3.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#On Device2, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Access. Configure gigabitethernet0/1 to allow services of VLAN2 to pass and configure gigabitethernet0/2 to allow services of VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet0/2
Device2(config-if-gigabitethernet0/2)#switchport mode access
Device2(config-if-gigabitethernet0/2)#switchport access vlan 3
Device2(config-if-gigabitethernet0/2)#exit
```

#On Device2, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN2 and VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#switchport mode trunk
Device2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2-3
Device2(config-if-gigabitethernet0/3)#exit
```

Step 3: Check the result.

#Query the VLAN information on Device1.

```
Device1#show vlan 2
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Interface
---- ---- -------------------------------- ------- --------- -----------------------------
1    2    VLAN0002                         static  Tagged    gi0/3
                                                   Untagged  gi0/1
Device1#show vlan 3
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Interface
---- ---- -------------------------------- ------- --------- -----------------------------
1    3    VLAN0003                         static  Tagged    gi0/3
                                                   Untagged  gi0/2
```

#Query the VLAN information on Device2.

```
Device2#show vlan 2
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Interface
---- ---- -------------------------------- ------- --------- -----------------------------
1    2    VLAN0002                         static  Tagged    gi0/3
                                                   Untagged  gi0/1
Device2#show vlan 3
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Interface
---- ---- -------------------------------- ------- --------- -----------------------------
1    3    VLAN0003                         static  Tagged    gi0/3
                                                   Untagged  gi0/2
```

#PC1 and PC2 cannot communicate with each other, PC1 can access only Server1, and PC2 can access only Server2.

23.3.2 Configure MAC Address-Based VLANs *-B -S -E -A*

Network Requirements

- PC1 and PC2 can access the network through different ports of Device.
- The MAC-address based VLAN functions need to be configured so that the PCs with the specified MAC addresses can access the server through different ports. PCs which do not have a specified MAC address can access the server only through a specified port.

Network Topology

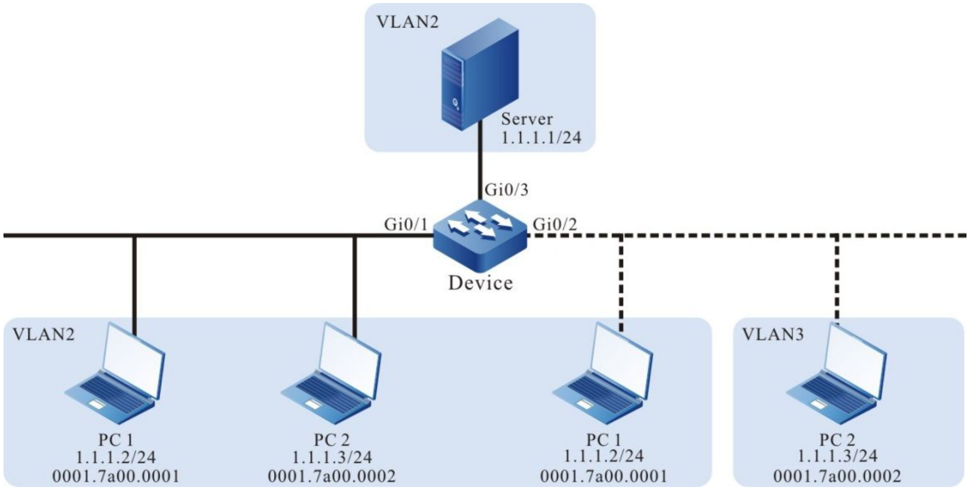


Figure 23-3 Networking for Configuring MAC address-Based VLANs

Configuration Steps

Step 1: On Device, configure VLANs, and configure the port link types of the ports.

#On Device, create VLAN2 and VLAN3.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device2, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/3 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#On Device, configure the link type of port gigabitethernet0/2 to Hybrid and allow services of VLAN2 and VLAN3 to pass, and set PVID to 3.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 3
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the MAC address-based VLAN function.

#On Device, configure an MAC address-based VLAN entry so that the packets with the source MAC address 94ae.e300.0001 can be forwarded in VLAN2.

```
Device(config)#mac-vlan mac-address 94ae.e300.0001 vlan 2
```

#On port gigabitethernet0/2 of Device, enable the MAC address-based VLAN function.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Check the result.

#On Device, query MAC VLAN entries and port enable status.

```
Device#show mac-vlan
                          total 4096,    used 1,    left 4095

---------------------------------MAC-VLAN---------------------------------
NO.   Mac Address     Dynamic Vlan  Static Vlan  Current Pri  Static Pri
----- --------------- ------------- ------------ ------------ -----------
1     94ae.e300.0001  0             2            0            0

-----------------------------ENABLE MAC-VLAN-----------------------------
gi0/2
```

#PC1 can access the server through port gigabitethernet0/1 or gigabitethernet0/2, while PC2 can access the server only through port gigabitethernet0/1.

23.3.3 Configure IP Subnet-Based VLANs *-B -S -E -A*

Network Requirements

- Server1 is the server in the office network, and Server2 is the server in the production network.
- The IP subnet-based VLAN functions need to be configured so that PC1 can access only Server1 and PC2 can access only Server2.

Network Topology

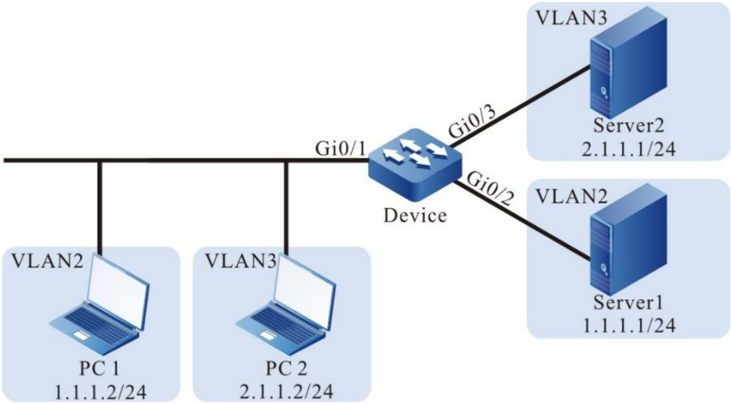


Figure 23-4 Configuring IP Subnet-Based VLANs

Configuration Steps

Step 1: On Device, configure VLANs, and configure the port link types of the ports.

#On Device, create VLAN2 and VLAN3.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device, configure the link type of port gigabitethernet0/1 to Hybrid and allow services of VLAN2 and VLAN3 to pass, and set PVID to 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode hybrid
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, configure the link type of ports gigabitethernet0/2 and gigabitethernet0/3 to Access. Configure gigabitethernet0/2 to allow services of VLAN2 to pass and configure gigabitethernet0/3 to allow services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

Step 2: Configure IP subnet-based VLAN functions.

#On Device, configure IP subnet-based VLAN entries so that the packets with the source IP address in the 2.1.1.0/24 subnet can be forwarded in VLAN3.

```
Device(config)#ip-subnet-vlan ipv4 2.1.1.0 mask 255.255.255.0 vlan 3
```

#On port gigabitethernet0/1 of Device, enable the IP subnet-based VLAN function.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip-subnet-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#On Device, query IP subnet VLAN entries and port enable status.

```
Device(config)#show ip-subnet-vlan
-------------------------IP-SUBNET-VLAN------------------------
NO.   IP                MASK              VLAN    PRI
------ ------------------ ------------------ ------- ----------
1     2.1.1.0           255.255.255.0     3       0

---------------------Enable SUBNET-VLAN----------------------
gi0/1

------------------Enable SUBNET-VLAN Priority------------------
```

#PC1 can access only Server1 and PC2 can access only Server2.

23.3.4 Configure Protocol-Based VLANs *-B -S -E -A*

Network Requirements

- PC is a host in the Ethernet, and Server1 and Server2 are two servers in the Ethernet.
- The protocol-based VLAN function needs to be configured so that the PC can access only Server 1 before the protocol-based VLAN function is enabled on the port of Device. After the protocol-based VLAN function is enabled on the port, PC can access only Server2.

Network Topology

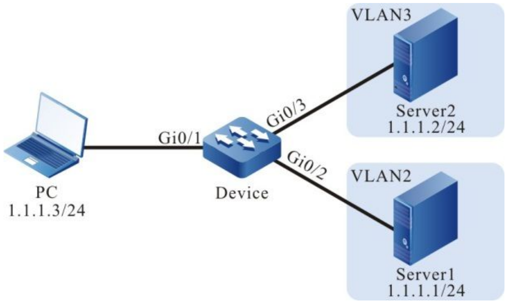


Figure 23-5 Networking for Configuring Protocol-Based VLANs

Configuration Steps

Step 1: On Device, configure VLANs, and configure the port link types of the ports.

#On Device, create VLAN2 and VLAN3.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#On Device, configure the link type of port gigabitethernet0/1 to Hybrid and allow services of VLAN2 and VLAN3 to pass, and set PVID to 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
```

#On Device, configure the link type of ports gigabitethernet0/2 and gigabitethernet0/3 to Access. Configure gigabitethernet0/2 to allow services of VLAN2 to pass and configure gigabitethernet0/3 to allow services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

Step 2: Configure the protocol-based VLAN function.

#On Device, configure a protocol profile for IP(0x0800) packets that are based on ETHERII encapsulation.

```
Device(config)#protocol-vlan profile 1 frame-type ETHERII ether-type 0x0800
```

#On port gigabitethernet0/1 of Device, the packets that match the protocol profile are forwarded in VLAN3, and the protocol VLAN function is enabled.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#protocol-vlan profile 1 vlan 3
Device(config-if-gigabitethernet0/1)#protocol-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#On Device, query protocol VLAN entries and port enable status.

```
Device#show protocol-vlan profile
--------------------PROTOCOL-VLAN-TEMPLATE------------------------
Profile   Frame-type     Ether-type
------------------------------------------------------------------
1         ETHERII        0x800

-----------------------Enable PROTOCOL-VLAN-----------------------
gi0/1

-------------------Enable PROTOCOL-VLAN Profile-------------------
gi0/1: total-profiles 1
       vlan 3, profile 1
Device#show protocol-vlan
---------------------------PROTOTOCL-VLAN-------------------------
Interface             Profile               VLAN
---------------------- --------------------- ---------------------
gi0/1                 1                     3

-----------------------Enable PROTOCOL-VLAN-----------------------
gi0/1

-------------------Enable PROTOCOL-VLAN Profile-------------------
gi0/1: total-profiles 1
       vlan 3, profile 1
```

#Before the protocol-based VLAN function is enabled on port gigabitethernet0/1, PC can access only Server1. After the protocol-based VLAN function is enabled on port gigabitethernet0/1, PC can access only Server2.

24 Super-VLAN

24.1 Overview

Different VLANs are isolated from each other at layer 2. To enable them to communicate with each other, you must configure a VLAN interface and IP address for each VLAN. However, this mode consumes a large number of scarce IP address resources. Super-VLAN, also called VLAN aggregation, can solve this problem effectively. A common VLAN, after being added into a super-VLAN, becomes a sub-VLAN of the super-VLAN. If the Address Resolution Protocol (ARP) proxy function is enabled for the super-VLAN, the super-VLAN shares its VLAN interface with its sub-VLANs. In this way, the sub-VLANs take the VLAN interface IP address of the super-VLAN as the gateway to implement layer-3 communication. This saves IP address resources.

24.2 Super-VLAN Function Configuration

Table 24-1 Super-VLAN Function List

Configuration Tasks	
Configure a super-VLAN.	Configure a super-VLAN.
Configure sub-VLAN members of the super-VLAN.	Configure sub-VLAN members of the super-VLAN.
Enable the ARP proxy function.	Enable the ARP proxy function.

24.2.1 Configure a Super-VLAN *-S -E -A*

Configuration Conditions

None

Configure a Super-VLAN

On a super-VLAN, a VLAN interface can be configured, but no port can be added. The created super-VLAN must not be an existing VLAN or sub-VLAN.

Table 24-2 Configuring a Super-VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create a super-VLAN.	**super-vlan** *vlan-id*	Mandatory. By default, no super-VLAN is created. After creating a super-VLAN, you will enter the super-VLAN configuration mode automatically.
Configure the description of a super-VLAN.	**description** *description*	Optional. By default, the description of a super-VLAN is "SuperVLAN*vlan-id", such as*SuperVLAN0100.

24.2.2 Configure Sub-VLAN Members of a Super-VLAN *-S -E -A*

Configuration Conditions

None

Configure Sub-VLAN Members of a Super-VLAN

One super-VLAN supports a maximum of 8 sub-VLAN members, and one VLAN can become the sub-VLAN member of only one super-VLAN. On a sub-VLAN, a VLAN interface cannot be configured but a port can be added into it. The method for adding a port into a sub-VLAN is the same as the method for adding a port into a common VLAN. The VLAN ID of a sub-VLAN must not be identical with the VLAN ID of an existing super-VLAN.

Table 24-3 Configuring Sub-VLAN Members of a Super-VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the super-VLAN configuration mode.	**super-vlan** *vlan-id*	-
Configure sub-VLAN members of the super-VLAN.	**sub-vlan** *vlan-list*	Mandatory. By default, a super-VLAN is not configured with sub-VLAN members.

24.2.3 Enable the ARP Proxy Function -S -E -A

Configuration Conditions

Before enabling the ARP proxy function, ensure that:

- The VLAN interface corresponding to the super-VLAN and the IP address have been configured.

Configure the ARP Proxy Function

After the ARP proxy function of a super-VLAN is configured, the sub-VLANs can communicate with each other at layer 3 through ARP proxy.

Table 24-4 Enabling the ARP Proxy Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the super-VLAN configuration mode.	**super-vlan** *vlan-id*	-
Enable the ARP proxy function.	**arp proxy enable**	Mandatory. By default, the ARP proxy function is disabled.

NOTE

- The ARP proxy function relies on the layer-3 forwarding function. If the device does not support the layer-3 forwarding function, the ARP proxy function does not take effect.

24.2.4 Super-VLAN Monitoring and Maintaining -S -E -A

Table 24-5 Super-VLAN Monitoring and Maintaining

Command	Description
show super-vlan [*vlan-id*]	Displays the information about the specified super-VLAN.

24.3 Super-VLAN Typical Configuration Example

24.3.1 Configure a Super-VLAN *-S -E -A*

Network Requirements

- PC1 and PC2 are two hosts in Sub-VLAN2, PC3 is a host in Sub-VLAN3, and Server is a server in VLAN5.
- The super-VLAN function has been configured on Device. Then, PC1 and PC2 can intercommunicate with each other at layer2. PC1 and PC2 can intercommunicate with PC3 at layer3, and they can access the server.

Network Topology

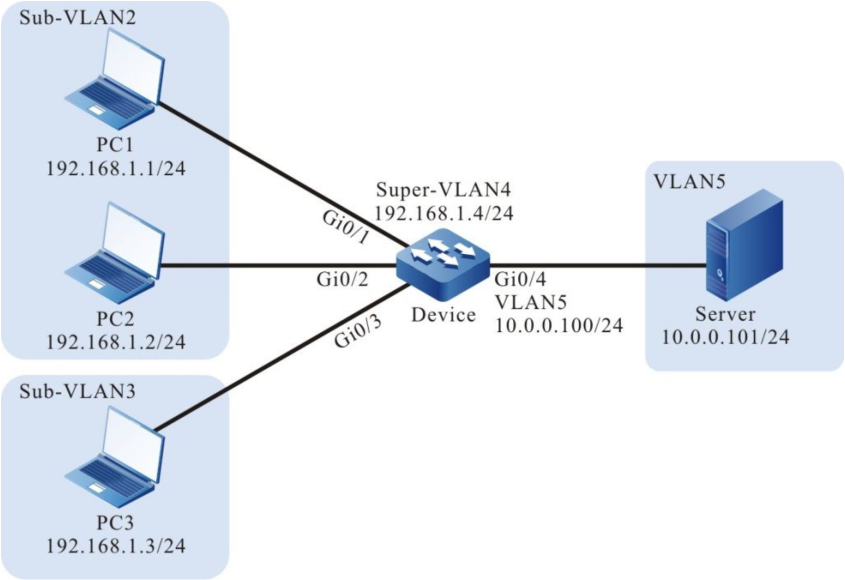


Figure 24-1 Networking for Configuring a Super-VLAN

Configuration Steps

Step 1: On Device, configure VLANs, and configure the port link types of the ports.

#On Device, create VLAN2-VLAN5.

```
Device#configure terminal
Device(config)#vlan 2-5
```

#On Device, set the IP address of VLAN interface 4 to 192.168.1.4 and the mask as 255.255.255.0, and set the IP address of VLAN interface 5 to 10.0.0.100 and the mask as 255.255.255.0.

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 192.168.1.4 255.255.255.0
Device(config-if-vlan4)#exit
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 10.0.0.100 255.255.255.0
Device(config-if-vlan5)#exit
```

#On Device, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#On Device, configure the link type of port gigabitethernet0/3 to Access and allow services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

#On Device, configure the link type of port gigabitethernet0/4 to Access and allow services of VLAN5 to pass.

```
Device(config)#interface gigabitethernet 0/4
Device(config-if-gigabitethernet0/4)#switchport mode access
Device(config-if-gigabitethernet0/4)#switchport access vlan 5
Device(config-if-gigabitethernet0/4)#exit
```

#Query the VLAN and port information of Device.

```
Device#show vlan 2
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Interface
---- ---- -------------------------------- ------- --------- -----------------------------
1    2    VLAN0002                         static  Untagged  gi0/1  gi0/2
Device#show vlan 3
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Interface
---- ---- -------------------------------- ------- --------- -----------------------------
1    3    VLAN0003                         static  Untagged  gi0/3
Device#show vlan 5
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Interface
---- ---- -------------------------------- ------- --------- -----------------------------
1    5    VLAN0005                         static  Untagged  gi0/4
```

Step 2: On Device, configure the super-VLAN function.

#On Device, configure VLAN4 as the super-VLAN, VLAN2 and VLAN3 as sub-VLANs, and enable ARP proxy.

```
Device(config)#super-vlan 4
Device(config-super-vlan4)#sub-vlan 2,3
Device(config-super-vlan4)#arp proxy enable
Device(config-super-vlan4)#exit
```

#Query the super-VLAN information of Device.

```
Device#show super-vlan
--------------------------------------------------------------------------------
NO.  SuperVlan  Description                Arp Proxy  SubVlan  Member
--------------------------------------------------------------------------------
1    4          SuperVLAN0004              enable     2-3
```

NOTE

- To enable the hosts in different sub-VLANs to communicate with each other at layer 3, the ARP proxy function must be enabled.

Step 3: Check the result. Use the ping command to check the connectivity between PC1, PC2, PC3 and the server.

#PC1 and PC2 in Sub-VLAN2 can ping each other successfully.

#PC1 and PC2 in Sub-VLAN2 and PC3 in Sub-VLAN3 can ping each other successfully.

#PC1, PC2, and PC3 in Sub-VLANs and the server can ping each other successfully.

25 Voice-VLAN

25.1 Overview

Voice-VLAN is a mechanism that provides security and Quality of Service (QoS) guarantee for voice data flows. In a network, usually two types of traffic coexists, voice data and service data. During transmission, voice data has a higher priority than service data so as to reduce delay and packet loss that may occur during the transmission process. Voice-VLAN can automatically recognize voice traffic and distribute the voice traffic to a specific VLAN with QoS guarantee.

25.2 Voice-VLAN Function Configuration

Table 25-1 Voice-VLAN Function List

Configuration Tasks	
Configure a voice-VLAN.	Configure a voice-VLAN.
Configure an OUI address.	Configure an OUI address.
Configure the aging time.	Configure the aging time of voice-VLAN entries.
Enable the voice-VLAN function of a port.	Enable the voice-VLAN function of a port.
Configure the voice-VLAN working mode on the port.	Configure a voice-VLAN to automatic mode.
	Configure a voice-VLAN to manual mode.

25.2.1 Configure a Voice-VLAN *-B -S -E -A*

A voice VLAN is used to transmit voice packets. The 802.1 priorities of the recognized voice packets are replaced with the priority of the voice-VLAN. Then the packets are distributed into the voice VLAN for forwarding. A device supports a maximum of one voice-VLAN.

Configuration Conditions

Before configuring a voice-VLAN, ensure that:

- The VLAN to be configured as a voice-VLAN has already been created.

Configure a Voice-VLAN

Table 25-2 Configuring a Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure a specified VLAN to voice-VLAN.	**voice vlan** *vlan-id* **cos** *priority*	Mandatory. By default, voice-VLAN is not configured, that is, the voice-VLAN function is not globally enabled.

25.2.2 Configure an OUI Address *-B -S -E -A*

Configuration Conditions

Before configuring an OUI address, ensure that:

- The voice-VLAN function is globally enabled.
- The voice-VLAN function is enabled on the port.

Configure an OUI Address

Organizationally Unique Identifiers (OUIs) are used to identify voice packets that are sent by voice devices of manufacturers. After a port that works in voice-VLAN automatic mode receives an Untag packet, it takes out the MAC address of the packet and performs the AND operation with the OUI mask. If the obtained address range is the same as the OUI address, it indicates that matching the OUI address succeeds, and the packet is recognized as a voice packet.

Table 25-3 Configuring an OUI Address

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure an OUI address.	**voice vlan oui-mac** *oui-mac-address* **mask** *mask* **name** *oui-name*	Mandatory. By default, five OUI addresses are available. A device supports a maximum of 16 OUI addresses.

25.2.3 Enable the Voice-VLAN Function *-B -S -E -A*

After the voice-VLAN function is enabled on a port, the port uses a method according to the voice-VLAN working mode to automatically recognize the received packets.

Configuration Conditions

Before enabling the voice-VLAN function of a port, ensure that:

- The voice-VLAN function has been globally enabled.
- The port has been added into the voice-VLAN.

Enable the Voice-VLAN Function of a Port

Table 25-4 Enabling the Voice-VLAN Function of a Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Enable the voice-VLAN function of a port.	**voice vlan enable**	Mandatory. By default, the voice-VLAN function is disabled on the port.

25.2.4 Configure the Voice-VLAN Working Mode on the Port *-B -S -E -A*

The voice-VLAN of a port can work in automatic mode or manual mode. The ports working in different voice-VLAN modes recognize voice packets in different ways.

- Automatic mode: If the packets received by the port are Untag packets and the source MAC address of the packets matches an OUI address, the packets are regarded as voice packets.

- Manual mode: If the packets received by the port are Untag packets, or Tag packets with the VLAN ID being the port PVID, the packets are regarded as voice packets.

Configuration Conditions

Before configuring the voice-VLAN working mode of a port, ensure that:

- The voice-VLAN function has been globally enabled.
- The voice-VLAN function of the port has been enabled.

Configure a Voice-VLAN to Automatic Mode

Table 25-5 Configuring a Voice-VLAN to Automatic Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port to work in voice-VLAN automatic mode.	**voice vlan mode auto**	Mandatory. By default, the port works in the voice-VLAN automatic mode.

Configure a Voice-VLAN to Manual Mode

Table 25-6 Configuring a Voice-VLAN to Manual Mode

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port to work in voice-VLAN manual mode.	**no voice vlan mode auto**	Mandatory. By default, the port works in the voice-VLAN automatic mode.

25.2.5 Configure Voice-VLAN Safety Mode *-B -S -E -A*

Network Requirements

- IP Phone and PC have accessed IP Network via the Device's port gigabitethernet0/1, the IP Phone's MAC address is 0001.0001.0001, the PC's MAC address is 0002.0002.0002.
- Configure Voice-VLAN safety mode on Device, so that IP Phone can access IP Network normally and PC cannot access IP Network.

Network Topology

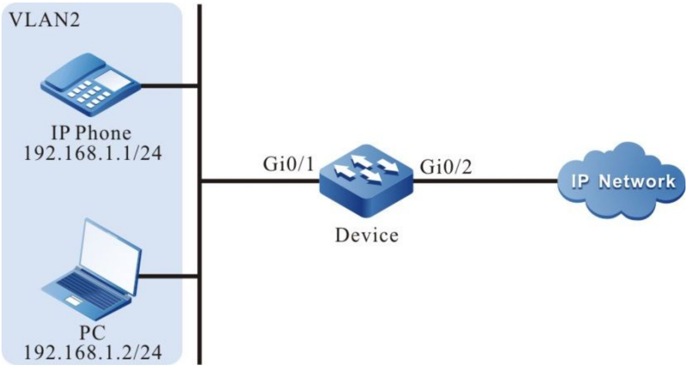


Figure 25-3 Networking diagram - Configure Voice-VLAN safety mode

Configuration steps

Step 1: On the Device, configure VLAN and the port link types.

#Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type gigabitethernet0/1 on Device to trunk to allow the pass of VLAN2 business.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the port link type gigabitethernet0/2 on Device to Trunk to allow the pass of VLAN2 business

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Voice-VLAN function.

#On the Device, configure VLAN2 to Voice-VLAN, and change corresponding Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On the Device, configure for globally enabling the Voice-VLAN safety mode.

```
Device(config)# voice vlan security enable
```

#On the Device's port gigabitethernet0/1, configure Voice-VLAN automatic mode.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#On the Device, configure the OUI address corresponding to the IP Phone's MAC address 0001.0001.0001.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#On the Device, check Voice-VLAN information.

```
Device#show voice vlan all
 Voice Vlan Global Information:  Voice Vlan enable
 Voice Vlan security:  enable
 Voice Vlan lldp-med authentication:  disable
 Voice Vlan VID: 2, Cos: 7
 Default OUI number: 5
 User config OUI number: 1
```

```
Voice vlan interface information:
 Interface          Mode
 -------------------------------------
 gi0/1              Auto-Mode

Voice Vlan OUI information: Total: 6
 MacAddr        Mask          Name
 ------------------------------------------------------------
 0001.0001.0000   ffff.ffff.0000   voice-vlan
 0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
 006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
 00d0.1e00.0000   ffff.ff00.0000   Pingtel-phone  default
 00e0.7500.0000   ffff.ff00.0000   Polycom-phone  default
 00e0.bb00.0000   ffff.ff00.0000   3Com-phone  default
```

Step 3: Check the result.

#The priority level of message 802.1P sent by the IP Phone to IP Network is changed to 7.

#The PC is denied access to the IP Network.

25.2.6 Configure Voice-VLAN lldp-med Authentication Mode *-B -S -E -A*

Network Requirements

- IP Phone (which can send LLDP message carrying voice field) and PC have accessed IP Network via the Device's port gigabitethernet0/1, the IP Phone's MAC address is 0001.0001.0001, the PC's MAC address is 0002.0002.0002.
- Configure Voice-VLAN lldp-med authentication mode on Device, so that IP Phone can access IP Network normally and PC cannot access IP Network.

Network Topology

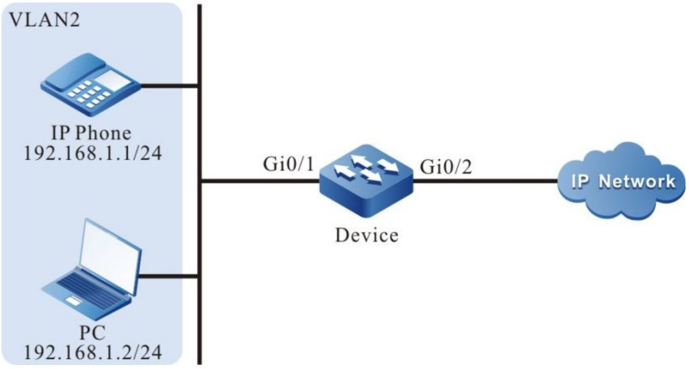


Figure 25-4 Networking diagram - Configure Voice-VLAN lldp-med authentication mode

Configuration steps

Step 1: On the Device, configure VLAN and the port link types.

#Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type gigabitethernet0/1 on Device to trunk to allow the pass of VLAN2 business.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the port link type gigabitethernet0/2 on Device to Trunk to allow the pass of VLAN2 business

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Voice-VLAN function.

#On the Device, configure VLAN2 to Voice-VLAN, and change corresponding Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On the Device, configure for globally enabling Voice-VLAN lldp-med authentication mode.

```
Device(config)#voice vlan lldp-med authentication
```

#On the Device's port gigabitethernet0/1, configure Voice-VLAN automatic mode.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#On the Device, configure the OUI address corresponding to the IP Phone's MAC address 0001.0001.0001.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#On the Device, check Voice-VLAN information.

```
Device#show voice vlan all
 Voice Vlan Global Information:  Voice Vlan enable
 Voice Vlan security:  disable
 Voice Vlan lldp-med authentication:  enable
 Voice Vlan VID: 2, Cos: 7
 Default OUI number: 5
 User config OUI number: 1

 Voice vlan interface information:
  Interface            Mode
  -------------------------------------
  gi0/1               Auto-Mode

 Voice Vlan OUI information: Total: 6
  MacAddr         Mask            Name
  -----------------------------------------------------------
  0001.0001.0000   ffff.ffff.0000   voice-vlan
  0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
  006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
  00d0.1e00.0000   ffff.ff00.0000   Pingtel-phone  default
  00e0.7500.0000   ffff.ff00.0000   Polycom-phone  default
  00e0.bb00.0000   ffff.ff00.0000   3Com-phone  default

 Voice Vlan lldp-med authenticated mac information:
  MacAddr         Interface
  -----------------------------------------------
0001.0001.0001   gi0/1
```

Step 3: Check the result.

#The priority level of message 802.1P sent by the IP Phone to IP Network is changed to 7.

#The PC is denied access to the IP Network.

25.2.7 Voice-VLAN Monitoring and Maintaining *-B -S -E -A*

Table 25-7 Voice-VLAN Monitoring and Maintaining

Command	Description
show voice vlan { **all** | **interface** [*interface-name*] | **link-aggregation** [*link-aggregation-id*] | **mac** [*mac-address*] | **oui** }	Displays the information about the voice-VLAN.

25.3 Voice-VLAN Typical Configuration Example

25.3.1 Configure a Voice-VLAN to Manual Mode

-B -S -E -A

Network Requirements

- IP Phone and PC can access IP Network through Device.
- The voice-VLAN in manual mode has been configured on Device. If the network is normal, IP Phone and PC can normally access IP Network. If the network is congested, IP Phone has a higher priority than PC in accessing IP Network.

Network Topology

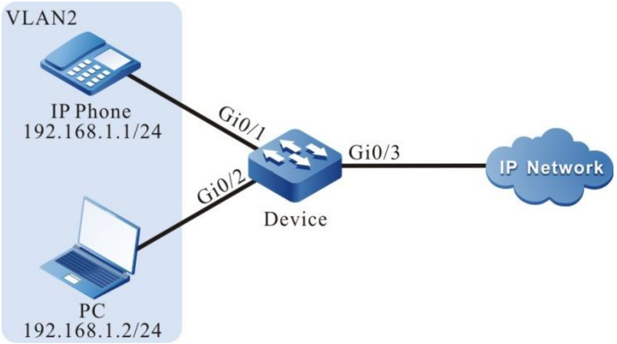


Figure 25-1 Networking for Configure a Voice-VLAN to Manual Mode

Configuration Steps

Step 1: Configure a VLAN, and configure the link type of the ports.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device2, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#On Device, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode trunk
Device(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/3)#exit
```

Step 2: Configure the voice-VLAN function.

#On Device, configure VLAN2 to voice-VLAN, and configure the Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On port gigabitethernet0/1 of Device, configure the voice-VLAN mode to manual mode.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#no voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, query the voice-VLAN information.

```
Device#show voice vlan all
 Voice Vlan Global Information:  Voice Vlan enable
 Voice Vlan VID: 2, Cos: 7
 Default OUI number: 5
 User config OUI number: 0
 Learned phone MAC address: 0
 Aging time: 1 minute

 Voice vlan interface information:
  Interface          Mode
  --------------------------------------
  gi0/1              Manual-Mode

 Voice Vlan OUI information: Total: 5
  MacAddr        Mask           Name
  ---------------------------------------------------------------
  0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
  006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
  00d0.1e00.0000   ffff.ff00.0000   Pingtel-phone  default
  00e0.7500.0000   ffff.ff00.0000   Polycom-phone  default
  00e0.bb00.0000   ffff.ff00.0000   3Com-phone  default

 Voice Vlan MAC information: Total: 0
       No any MAC enable
```

Step 3: Check the result.

#The 802.1 priority of the packets that are sent to IP Phone is modified to 7, and the 802.1P priority of the packets sent by PC to IP Network is not modified.

#When the network is normal, IP Phone and PC can normally access IP Network.

#If the network is congested, IP Phone can access IP Network with a priority higher than PC.

25.3.2 Configure a Voice-VLAN to Automatic Mode *-B -S -E -A*

Network Requirements

- IP Phone and PC access IP Network through port gigabitethernet0/1 of Device. The MAC address of IP Phone is 0001.0001.0001, and the MAC address of PC is

0002.0002.0002.

- The voice-VLAN in automatic mode has been configured. In this way, if the network is normal, IP Phone and PC can normally access IP network. If the network is congested, IP Phone has a higher priority than PC in accessing IP Network.

Network Topology

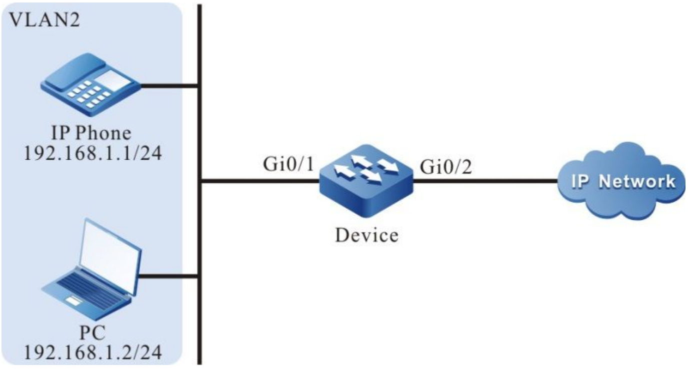


Figure 25-2 Networking for Configure a Voice-VLAN to Automatic Mode

Configuration Steps

Step 1: Configure a VLAN, and configure the link type of the ports.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device, configure the link type of port gigabitethernet0/1 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the voice-VLAN function.

#On Device, configure VLAN2 to voice-VLAN, and modify the Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On port gigabitethernet0/1 of Device, configure the voice-VLAN mode to automatic mode.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, configure the OUI address corresponding to the MAC address 0001.0001.0001 of IP Phone.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#On Device, query the voice-VLAN information.

```
Device#show voice vlan all
```

```
Voice Vlan Global Information:  Voice Vlan enable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 1
Learned phone MAC address: 0
Aging time: 1 minute

Voice vlan interface information:
 Interface            Mode
 --------------------------------------
 gi0/1               Auto-Mode

Voice Vlan OUI information: Total: 6
 MacAddr         Mask            Name
 -------------------------------------------------------------
 0001.0001.0000   ffff.ffff.0000   voice-vlan
 0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
 006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
 00d0.1e00.0000   ffff.ff00.0000   Pingtel-phone  default
 00e0.7500.0000   ffff.ff00.0000   Polycom-phone  default
 00e0.bb00.0000   ffff.ff00.0000   3Com-phone  default

Voice Vlan MAC information: Total: 0
      No any MAC enable
```

Step 3: Check the result.

#The 802.1 priority of the packets that are sent to IP Phone is modified to 7, and the 802.1P priority of the packets sent by PC to IP Network is not modified.

```
Device#show voice vlan mac

Voice Vlan MAC information: Total: 1

 MacAddr         Vid    Interface            AgeTime(min)
 -------------------------------------------------------------
 0001.0001.0001   2    gi0/1                 0
```

#When the network is normal, IP Phone and PC can normally access IP Network.

#If the network is congested, IP Phone can access IP Network with a priority higher than PC.

25.3.3 Configure Voice-VLAN Safety Mode *-B -S -E -A*

Network Requirements

- IP Phone and PC have accessed IP Network via the Device's port gigabitethernet0/1, the IP Phone's MAC address is 0001.0001.0001, the PC's MAC address is 0002.0002.0002.
- Configure Voice-VLAN safety mode on Device, so that IP Phone can access IP Network normally and PC cannot access IP Network.

Network Topology

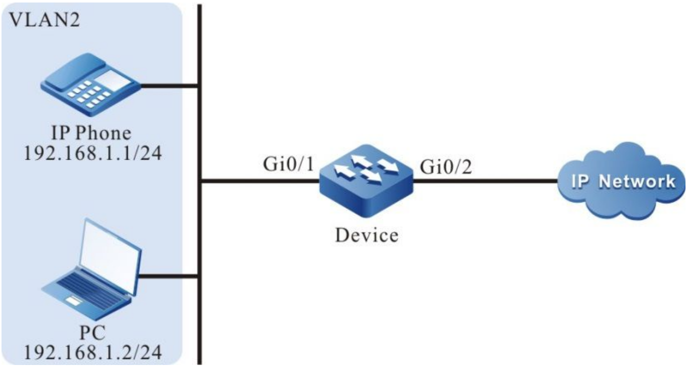


Figure 25-3 Networking diagram - Configure Voice-VLAN safety mode

Configuration steps

Step 1: On the Device, configure VLAN and the port link types.

#Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type gigabitethernet0/1 on Device to trunk to allow the pass of VLAN2 business.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the port link type gigabitethernet0/2 on Device to Trunk to allow the pass of VLAN2 business

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Voice-VLAN function.

#On the Device, configure VLAN2 to Voice-VLAN, and change corresponding Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On the Device, configure for globally enabling the Voice-VLAN safety mode.

```
Device(config)# voice vlan security enable
```

#On the Device's port gigabitethernet0/1, configure Voice-VLAN automatic mode.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#On the Device, configure the OUI address corresponding to the IP Phone's MAC address 0001.0001.0001.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#On the Device, check Voice-VLAN information.

```
Device#show voice vlan all
 Voice Vlan Global Information:  Voice Vlan enable
 Voice Vlan security:  enable
 Voice Vlan lldp-med authentication:  disable
 Voice Vlan VID: 2, Cos: 7
 Default OUI number: 5
 User config OUI number: 1

 Voice vlan interface information:
  Interface            Mode
  --------------------------------------
  gi0/1               Auto-Mode

 Voice Vlan OUI information: Total: 6
  MacAddr         Mask            Name
  --------------------------------------------------------------
  0001.0001.0000   ffff.ffff.0000   voice-vlan
  0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
  006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
  00d0.1e00.0000   ffff.ff00.0000   Pingtel-phone  default
  00e0.7500.0000   ffff.ff00.0000   Polycom-phone  default
  00e0.bb00.0000   ffff.ff00.0000   3Com-phone  default
```

Step 3:   Check the result.

#The priority level of message 802.1P sent by the IP Phone to IP Network is changed to 7.

#The PC is denied access to the IP Network.

25.3.4 Configure Voice-VLAN lldp-med Authentication Mode *-B -S -E -A*

Network Requirements

- IP Phone (which can send LLDP message carrying voice field) and PC have accessed IP Network via the Device's port gigabitethernet0/1, the IP Phone's MAC address is 0001.0001.0001, the PC's MAC address is 0002.0002.0002.
- Configure Voice-VLAN lldp-med authentication mode on Device, so that IP Phone

can access IP Network normally and PC cannot access IP Network.

Network Topology

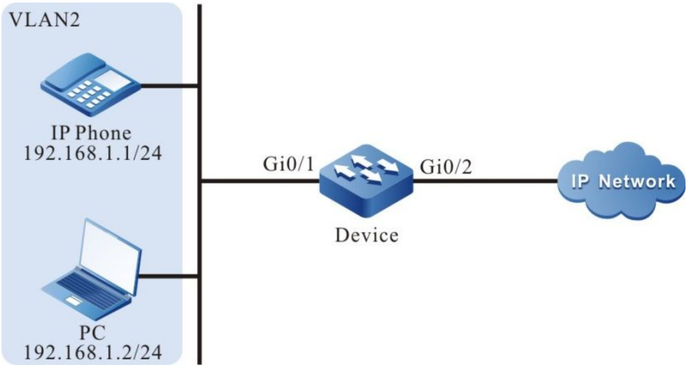


Figure 25-4 Networking diagram - Configure Voice-VLAN lldp-med authentication mode

Configuration steps

Step 1: On the Device, configure VLAN and the port link types.

#Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type gigabitethernet0/1 on Device to trunk to allow the pass of VLAN2 business.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the port link type gigabitethernet0/2 on Device to Trunk to allow the pass of VLAN2 business

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Voice-VLAN function.

#On the Device, configure VLAN2 to Voice-VLAN, and change corresponding Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On the Device, configure for globally enabling Voice-VLAN lldp-med authentication mode.

```
Device(config)#voice vlan lldp-med authentication
```

#On the Device's port gigabitethernet0/1, configure Voice-VLAN automatic mode.

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#On the Device, configure the OUI address corresponding to the IP Phone's MAC address 0001.0001.0001.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#On the Device, check Voice-VLAN information.

```
Device#show voice vlan all
 Voice Vlan Global Information:  Voice Vlan enable
 Voice Vlan security:  disable
 Voice Vlan lldp-med authentication:  enable
 Voice Vlan VID: 2, Cos: 7
 Default OUI number: 5
 User config OUI number: 1

 Voice vlan interface information:
  Interface          Mode
  -------------------------------------
  gi0/1              Auto-Mode

 Voice Vlan OUI information: Total: 6
  MacAddr        Mask           Name
  -----------------------------------------------------------
  0001.0001.0000   ffff.ffff.0000   voice-vlan
  0003.6b00.0000   ffff.ff00.0000   Cisco-phone  default
  006b.e200.0000   ffff.ff00.0000   H3C-Aolynk-phone  default
  00d0.1e00.0000   ffff.ff00.0000   Pingtel-phone  default
  00e0.7500.0000   ffff.ff00.0000   Polycom-phone  default
  00e0.bb00.0000   ffff.ff00.0000   3Com-phone  default

 Voice Vlan lldp-med authenticated mac information:
  MacAddr        Interface
  -----------------------------------------------
0001.0001.0001   gi0/1
```

Step 3: Check the result.

#The priority level of message 802.1P sent by the IP Phone to IP Network is changed to 7.

#The PC is denied access to the IP Network.

26 MAC Address Table Management

26.1 Overview

A MAC address entry consists of the MAC address of a terminal, the device port that is connected to the terminal, and the ID of the VLAN to which the port belongs. After a device receives a datagram, it matches the destination MAC address of the packet with the MAC address table entries that are saved in the device so as to locate a packet forwarding port efficiently.

MAC addresses are categorized into two types: dynamic MAC addresses and static MAC addresses. Static MAC addresses are categorized into static forwarding MAC addresses and static filtering MAC addresses.

Dynamic MAC address learning is the basic MAC address learning mode of the devices. Each dynamic MAC address entry has aging time. If no packet whose source MAC address matches a MAC address entry is received by the corresponding VLAN and port, the device deletes the MAC address entry.

The dynamic MAC address learning/forwarding process is as follows:

- When a device receives a packet, it searches the MAC address table of the corresponding VLAN for the MAC address entry that matches the source MAC address of the packet. If no corresponding matching entry is available, the source MAC address of the packet is written into the MAC address table, and the aging time timer of the new MAC address entry is started. If a matching MAC address entry is found, the aging time of the MAC address entry is updated.
- In the corresponding VLAN, the device searches the MAC address table for MAC address entry that matches the destination MAC address of the packet. If no matching entry is available, the packet is flooded to the other ports with the same VLAN ID. If a matching MAC address entry is available, the packet is forwarded through the specified port.

Static filtering MAC addresses are used to isolate devices which are aggressive, preventing the devices from communicating with external devices.

The configuration/forwarding process of static filtering MAC addresses is as follows:

- Static filtering MAC addresses can only be configured by users.
- If the source MAC address or destination MAC address of a packet matches a static filtering MAC address entry in the corresponding VLAN, the packet is discarded.

Static forwarding MAC addresses are used to control the routing principle of packets, and prevent frequent MAC address migration of MAC address entries in the table. MAC address migration means that: A device learns a MAC address from port A, then the device receives packets whose source MAC address is the same as the MAC address from port B, and port B and port A belong to the same VLAN. At this time, the forwarding port saved in the MAC address entry is updated from port A to port B.

The configuration/forwarding process of static forwarding MAC addresses is as follows:

- Static forwarding MAC addresses are configured by users.
- If the destination MAC address of a packet matches a static MAC address entry in

the corresponding VLAN, the packet is forwarded through the specified port.

One port can learn the same MAC address from different VLANs, but one MAC address can only be learnt by one port in one VLAN.

26.2 MAC Address Management Function Configuration

Table 26-1 MAC Address Management Function List

Configuration Tasks	
Configure management properties of MAC addresses.	Configure the MAC address aging time.
	Configure the MAC address learning capability.
Configure limitations on MAC address learning.	Configure limitations on port-based dynamic MAC address learning.
	Configure limitations on VLAN-based dynamic MAC address learning.
	Configure limitations on system-based dynamic MAC address learning.
Configure static MAC addresses.	Configure static filtering MAC addresses.
	Configure static forwarding MAC addresses that are bound to a port.
	Configure static forwarding MAC addresses that are bound to an aggregation group.

26.2.1 Configure Management Properties of MAC Addresses *-B -S -E -A*

MAC address management properties include: MAC address aging time, and the MAC address learning capability of ports.

Each dynamic MAC address entry has aging time. If no packet whose source MAC address matches a MAC address entry is received by the specified VLAN, the device deletes the MAC address entry. If the specified VLAN receives a packet whose source MAC address matches a MAC address entry, the device resets the aging time of the MAC address entry.

Static MAC addresses can only be configured and deleted by users, so static MAC addresses cannot age.

If devices in the network have idle ports and the ports do not allow free use, then the MAC address learning capability can be disabled on the port. Then, the packets received by the port will all be discarded. In this way, these ports cannot access the network, and hence the security of the network is improved.

Configuration Conditions

None

Configure the MAC Address Aging Time

The dynamic MAC address aging time set in a device takes effect globally. The value range of the MAC address aging time is:

- 0: MAC addresses do not age, that is, the learned dynamic MAC addresses do not age.
- 10-1000000: Aging time of dynamic MAC addresses. Unit: second. Default: 300.

If the aging time is configured too long, the MAC address table in the device may contain a large number of MAC address entries that are no long in use. In this way, the large number of invalid entries may use up MAC address resources, and new valid MAC address entries fail to be added to the device. If the aging time is configured too short, the device may frequently delete valid MAC address entries, affecting the device forwarding performance. Therefore, you need to configure a reasonable value for the aging time according to the actual environment.

Table 26-2 Configuring the MAC Address Aging Time

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Configure the MAC address aging time.	**mac-address aging-time** *aging-time-value*	Mandatory. By default, the MAC address aging time is set to 300 seconds.

Configure the MAC Address Learning Capability

MAC address learning capability can be enabled and disabled only for dynamic MAC address learning. By default, the MAC address learning capability is enabled on a port. Then the port learns MAC address entries and forwards corresponding packets. If the MAC address learning capability is enabled on a port, the port does not learn dynamic MAC addresses, and the received packets are discarded.

Table 26-3 Configuring the MAC Address Learning Capability

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected.

Step	Command	Description
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enable the MAC address learning capability on a port or aggregation group.	**mac-address learning**	Mandatory. By default, the MAC address learning capability is enabled on a port.

26.2.2 Configure Limitations on MAC Address Learning *-B -S -E -A*

Limitations on MAC address learning are categorized into three types: limitations on port-based dynamic MAC address learning, limitations on VLAN-based dynamic MAC address learning, and limitations on system-based MAC address learning.

If a large number of dynamic MAC address entries have been learned by the device, it takes a long time for the device to search the MAC address table before forwarding packets, and this may cause degradation of the device performance. Therefore, you can configure limitations on dynamic MAC address learning to improve the device performance. If you configure limitations on dynamic MAC address learning on a port or VLAN, the number of access terminals can be controlled.

Configuration Conditions

None

Configure Limitations on Port-Based Dynamic MAC Address Learning

If the number of MAC address entries that have been learned by a port has reached the threshold value, the port discards the packets whose source MAC addresses are not in the MAC address forwarding table.

Table 26-4 Configuring Limitations on Port-Based Dynamic MAC Address Learning

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-

Step	Command	Description
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure limitations on port-based dynamic MAC address learning.	**mac-address max-mac-count** *max-mac-count-value*	Mandatory. By default, there are no limitations on dynamic MAC address learning on a port. The value range of the threshold of dynamic MAC address learning is 1-32767.

NOTE

- In configuring limitations on port-based dynamic MAC address learning, if the configured threshold value is smaller than the number of existing dynamic MAC address entries on the port, the device prompts to manually clear some existing dynamic MAC address entries. After the MAC addresses are cleared, the configuration takes effect immediately.

Configure Limitations on VLAN-Based Dynamic MAC Address Learning

If the number of MAC address entries that have been learned by a specified VLAN has reached the threshold value, the VLAN discards the packets whose source MAC addresses are not in the MAC address forwarding table.

Table 26-5 Configuring Limitations on VLAN-Based Dynamic MAC Address Learning.

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Configure limitations on VLAN-based dynamic MAC address learning.	**mac-address vlan** *vlan-id* **max-mac-count** *max-mac-count-value*	Mandatory. By default, there are no limitations on dynamic MAC address learning in a VLAN. The value range of the threshold of dynamic MAC address learning is 1-32767.

NOTE

- In configuring limitations on VLAN-based dynamic MAC address learning, if the configured threshold value is smaller than the number of existing dynamic MAC address entries in the current VLAN, the device prompts to manually clear some existing dynamic MAC address entries. After the MAC addresses are cleared, the configuration takes effect immediately.

Configure Limitations on System-Based Dynamic MAC Address Learning

If the number of MAC address entries that have been learned by the system has reached the threshold value, the system discards the packets whose source MAC addresses are not in the MAC address forwarding table.

Table 26-6 Configuring Limitations on System-Based Dynamic MAC Address Learning

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Configure limitations on system-based dynamic MAC address learning.	**mac-address system max-mac-count** *max-mac-count-value*	Mandatory. By default, there are no limitations on dynamic MAC address learning. The value range of the threshold of dynamic MAC address learning is 1-32767.

NOTE

- In configuring limitations on system-based dynamic MAC address learning, if the configured threshold value is smaller than the number of existing dynamic MAC address entries in the current system, the device prompts to manually clear some existing dynamic MAC address entries. After the MAC addresses are cleared, the configuration takes effect immediately.

26.2.3 Configure Static MAC Addresses *-B -S -E -A*

Static MAC addresses are categorized into two types: static forwarding MAC addresses and static filtering MAC addresses.

The configured MAC addresses must be legal unicast MAC addresses instead of broadcast, multicast, or all-0 addresses.

One MAC address can only be configured as a static forwarding MAC address or a static filtering MAC address in a VLAN.

Configuration Conditions

None

Configure Static Filtering MAC Addresses

After static filtering MAC address entries are configured, if the source or destination MAC addresses of the packets that are received by the corresponding VLAN match static filtering MAC address entries, the packets are discarded. This function prevents trustless devices from accessing the network, and prevents fraud and attacking activities of illegal users.

Table 26-7 Configuring Static Filtering MAC Addresses

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Configure static filtering MAC addresses.	**mac-address static** *mac-address-value* **vlan** *vlan-id* **drop**	Mandatory. By default, a device is not configured with static filtering MAC addresses.

Configure Static Forwarding MAC Addresses That Are Bound to a Port

With static forwarding MAC address entries configured, after the corresponding VLAN receives packets, the port matches the destination MAC addresses of the packets with the static forwarding MAC address entries that are configured on the device. If they match successfully, the device forwards the packets through the specified port. This function helps to control the routing principle of packets more flexibly, and prevents frequent migration of MAC address entries in the table.

Table 26-8 Configuring Static Forwarding MAC Addresses That Are Bound to a Port

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Configure static forwarding MAC addresses that are bound to a port.	**mac-address static** *mac-address-value* **vlan** *vlan-id* **interface** *interface-name*	Mandatory. By default, a device is not configured with static forwarding MAC addresses.

Configure Static Forwarding MAC addresses That Are Bound to an Aggregation Group

With static forwarding MAC address entries configured, after the aggregation group receives packets, the port matches the destination MAC addresses of the packets with the static forwarding MAC address entries that are configured on the device. If they match successfully, the device forwards the packets through the specified aggregation group. This function helps to control the routing principle of packets more flexibly, and prevents frequent migration of MAC address entries in the table.

Table 26-9 Configuring Static Forwarding MAC Addresses That Are Bound to an Aggregation Group

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Configure static forwarding MAC addresses that are bound to an aggregation group.	**mac-address static** *mac-address-value* **vlan** *vlan-id* **link-aggregation** *link-aggregation-id*	Mandatory. By default, a device is not configured with static forwarding MAC addresses.

NOTE

- Before configuring the command, ensure that the specified aggregation group has been created.

26.2.4 MAC Address Management Monitoring and Maintaining *-B -S -E -A*

Table 26-10 MAC Address Management Monitoring and Maintaining

Command	Description
clear mac-address dynamic { *mac-address-value* **| all | interface** *interface-list* | **link-aggregation** *link-aggregation-id* **| vlan** *vlan-id* [*mac-address-value* | **interface** *interface-list* | **link-aggregation** *link-aggregation-id*] }	Clears the MAC address entries that are dynamically learned.
show mac-address interface *interface-list* { **all** | **dynamic** | **static** [**config**] }	Displays MAC address entries on a port.
show mac-address link-aggregation *link-aggregation-id* { **all** | **dynamic** | **static** [**config**] }	Displays MAC address entries in an aggregation group.
show mac-address vlan *vlan-id* { **all** | **dynamic** | **static** [**config**] }	Displays MAC address entries in a VLAN.
show mac-address drop [*mac-address-value* | **config**]	Displays static filtering MAC address entries in the system.
show mac-address dynamic [*mac-address-value*]	Displays dynamic MAC address entries in the system.
show mac-address global learning	Displays whether the global MAC address learning capability is globally enabled in the system.
show mac-address static [*mac-address-value* **| config**]	Displays static forwarding MAC address entries in the system.
show mac-address system-mac	Displays the MAC address of the system.
show mac-address { *mac-address-value* **| all** }	Displays the information about the system MAC address entries or a specified MAC address entry.
show mac-address aging-time	Displays the aging time of dynamic MAC address entries.

Command	Description
show mac-address max-mac-count { **interface** [*interface-name*] | **link-aggregation** [*link-aggregation-id*] | **system** | **vlan** { *vlan-id* | **all** } }	Displays limitations on dynamic MAC address learning in the system.
show mac-address count [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **vlan** *vlan-id*]	Displays MAC address entry statistics in the system.

26.3 Configuration of MAC Address Migration Log Function

6.3.1 Configuration of MAC Address Migration Log Function *-B -S -E -A*

MAC address migration log function can be turned on and turned off manually; once MAC address migration log function is turned on, when address migration of MAC address table entry happens, a corresponding address migration log will be recorded.

Configuration Conditions

None

Turn on MAC address Migration Log Function

Table 26-11 Turn on MAC Address Migration Log Function

Steps	Command	Description
Enter global configuration mode	**config terminal**	-
Turn on address migration log function	**mac-address move log**	Turned on by default

Disable MAC Address Migration Log Function

Table 26-12 Disable MAC Address Migration Log Function

Steps	Command	Description
Enter global configuration mode	**config terminal**	-

Steps	Command	Description
Disable address migration log function	**no mac-address move log**	Once address migration log function is disabled, when address migration of MAC address table entry happens, log information will no longer be recorded.

26.3.2 Monitoring and Maintaining of MAC Address Migration Log Function *-B -S -E -A*

Table 26-13 Monitoring and Maintenance of MAC Address Migration

Command	Description
clear mac-address move log{*mac-address***}**	Erase MAC address migration log
show mac-address move config	Check the configuration information of MAC address migration log function.
show mac-address move log {*mac-address-value* **| count** *count* **| hardlearn | start-time** [*time*] **end-time** [*time*] **}**	Check the MAC address migration log.

27 STP

27.1 Overview

IEEE 802.1D defines the standard Spanning Tree Protocol (STP) to eliminate network loops, preventing data frames from circulating or multiplying in loops, which may result in network congestion and affect normal communication in the network. Through the STP algorithm, STP can determine where loops may exist in a network, block ports on redundant links, and trim the network into a tree structure in which no loops exist to prevent devices from receiving duplicated data frames. When the active path is faulty, STP recovers the connectivity of the blocked redundant links to ensure normal services. On the basis of STP, Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) are developed. The basic principles of the three protocols are the same, while RSTP and MSTP are improved versions of STP.

In STP, the following basic concepts are defined:

- Root bridge: Root of the finally formed tree structure of a network. The device with the highest priority acts as the root bridge.
- Root Port (RP): The port which is nearest to the root bridge. The port is not on the root bridge, and it communicates with the root bridge.
- Designated bridge: If the device sends Bridge Protocol Data Unit (BPDU) configuration information to a directly connected device or directly connected LAN, the device is regarded as the designated bridge of the directly connected device or directly connected LAN.
- Designated port: The designated bridge forwards BPDU configuration information through the designated port.
- Path cost: It indicates the link quality, and it is related to the link rate. Usually, a higher link rate means a smaller path cost, and the link is better.

The devices that run STP implement calculation of the STP by exchanging BPDU packets, and finally form a stable topology structure. BPDU packets are categorized into the following two types:

- Configuration BPDUs: They are also called BPDU configuration messages which are used to calculate and maintain the STP topology.
- Topology Change Notification (TCN) BPDUs: When the network topology structure changes, they are used to inform other devices of the change.

BPDU packets contain information that is required in STP calculation. The major information includes:

- Root bridge ID: It consists of the root bridge priority and the MAC address.
- Root path cost: It is the minimum path cost to the root bridge.
- Designated bridge ID: It consists of the designated bridge priority and the MAC address.
- Designated port ID: It consists of the designated port priority and port number.
- Message Age: Life cycle of BPDU configuration messages while they are broadcast in a network.

- Hello Time: Transmitting cycle of BPDU configuration messages.
- Forward Delay: Delay in port status migration.
- Max Age: Maximum life cycle of configuration messages in a device.

The election process of STP is as follows:

- Initial status.

The local device takes itself as the root bridge to generate BPDU configuration messages and sends the messages. In the BPDU packets, the root bridge ID and designated bridge ID are the local bridge ID, and root path cost is 0, and the specified port is the transmitting port.

Each port of the device generates a port configuration message which is used for STP calculation. In the port configuration message, the root bridge ID and the designated bridge ID are the local bridge ID, the root path cost is 0, and the specified port is the local port.

- Update port configuration messages.

After the local device receives a BPDU configuration message from another device, it compares the message with the port configuration message of the receiving port. If the received configuration message is better, the device uses the received BPDU configuration message to replace the port configuration message. If the port configuration message is better, the device does not perform any operation.

The principle of comparison is as follows: The root bridge IDs, root path cost, designated bridge IDs, designated port IDs, and receiving port IDs should be compared in order. The smaller value is better. If the values of previous item are the same, compare the next item.

- Select the root bridge.

The device that sends the optimal configuration message in the entire network is selected as the root bridge.

- Select port roles and port status.

All ports of the root bridge are designated ports, and the ports are in the Forwarding status. The designated bridge selects the optimal port configuration message from all ports. The receiving port of the message is selected as the root port, and the root port is in the Forwarding status. The other ports calculate designated port configuration messages according to the root port configuration message.

The calculation method is as follows: The root bridge ID is the route ID of the root port configuration message, the root path cost is the sum of the root path cost of the root port configuration message and the root port path cost, the designated bridge ID is the bridge ID of the local device, and the designated port is the local port.

Based on the port configuration message and the calculated designated port configuration message, determine port rules: If the designated port configuration message is better, the local port is selected as the designated port, and the port is in the Forwarding status. Then, the port configuration message is replaced by the designated port configuration message, and the designated port sends port configuration messages periodically at the interval of Hello Time. If the port configuration message is better, the port is blocked. The port is then in the Discarding status, and the port configuration message is not modified.

After the root bridge, root port, and designated port are selected, the tree structure network topology is set up successfully. Only the root port and the designated port can forward data. The other ports are in the Discarding status. They can only receive configuration messages but cannot send configuration messages or forward data.

If the root port of a non-root bridge fails to receive configuration messages periodically, the active path is regarded as faulty. The device re-generates a BPDU configuration message and TCN BPDU with itself as the root bridge and sends the messages. The messages causes re-calculation of the STP and then a new active path is obtained.

Before receiving new configuration messages, the other devices do not find the network topology change, so their root ports and designated port still forward data through the original path. The newly selected root port and designated port migrate to the Forwarding status after two Forward Delay periods to ensure that the new configuration message has been broadcast to the entire network and prevent occurrence of temporary loops that may be caused if both old and new root ports and designate ports forward data.

RSTP defined in IEEE 802.1w is developed based on STP, and it is the improved version of STP. RSTP realizes fast migration of port status and hence shortens the time required for a network to set up stable topology. RSTP is improved in the following aspects:

- It sets a backup port, that is, alternate port, for the root port. If the root port is blocked, the alternate port can fast switch over to become a new root port.
- It sets a backup port, that is, backup port, for the designated port. If the designated port is blocked, the backup port can fast switch over to become a new designated port.
- In a point-to-point link of two directly-connected devices, the designated port can enter the Forwarding status without delay only after a handshake with the downstream bridge.
- Some ports are not connected to the other bridges or shared links, instead, they are directly connected with user terminals. These ports are defined as edge ports. The status changes of edge ports do not affect the network connectivity, so the ports can enter the Forwarding status without delay.

However, both RSTP and STP form a single STP, which has the following shortages:

- Only one STP is available in the entire network. If the network size is large, the network convergence takes a long time.
- Packets of all VLANs are forwarded through one STP, therefore no load balancing is achieved.

MSTP defined in IEEE 802.1s is an improvement of STP and RSTP, and it is backward compatible with STP and RSTP. MSTP introduces the concept of region and instance. MSTP divides a network into multiple regions. Each region contains multiple instances, one instance can set up mapping with one or more VLANs, and one instance corresponds to one STP. One port may have different port role and status in different instances. In this way, packets of different VLANs are forwarded in their own paths.

In MSTP, definition of the following concepts is added:

- MST region: It consists of multiple devices in the switching network and the network between the devices. The devices in an MST region must meet the following requirements: The STP function has been enabled on the devices. They have the same MST region, MSTP level, and VLAN mapping table. They are directly connected physically.
- Internal Spanning Tree (IST): It is the STP of instance 0 in each region.
- Common Spanning Tree (CST): If each MST region is regarded as a device, then the STPs that connect MST regions are CSTs.
- Common and Internal Spanning Tree (CIST): It consists of the ISTs of MST regions and the CSTs between the MST regions. It is a single STP that connects all devices in the network.

- Multiple Spanning Tree Instance (MST Instance): STPs in MST regions. Each instance has an independent MST Instance.
- Common root: CIST root.
- Region root: Root of each IST and MST Instance in MST regions. In MST domains, each instance has an independent STP, so the region roots may be different. The root bridge of instance 0 is the region root of the region.
- Region edge ports: They are located at the edge of an MST region and they are used to connect ports of different MST regions.
- External path cost: It is the minimum path cost from a port to the common root.
- Internal path cost: It is the minimum path cost from a port to the region root.
- Master port: It is the region edge port with the minimum path cost to the common root in an MST region. The role of a master port in an MST Instance is the same as its role in a CIST.

The election rule of MSTP is similar to that of STP, that is, electing the bridge with the highest priority in the network as the root bridge of CIST by comparing configuration messages. Each MST region calculates its IST, and MST regions calculate CSTs, and all of the constructs CIST in the entire network. Based on mapping between VLANs and STP instances, each MST region calculates an independent STP MST Instance for each instance.

27.2 STP Function Configuration

Table 27-1 STP Function List

Configuration Tasks	
Configure basic functions of an STP.	Enable the STP function.
	Configure MST regions.
Configure bridge properties.	Configure the priority of a bridge.
	Configure Hello Time.
	Configure Forward Delay.
	Configure Max Age.
	Configure the maximum number of hops in an MST region.
Configure STP port properties.	Configure the priority of a port.
	Configure the default path cost standard for a port.
	Configure the path cost of a port.

Configuration Tasks	
	Configure the maximum transmitting rate of BPDU packets.
	Configure the timeout factor of BPDU packets.
	Configure an edge port.
	Configure the port link type.
Configure the working mode of an STP.	Configure the working mode of an STP.
Configure the STP protection function.	Configure the BPDU Guard function.
	Configure the BPDU Filter function.
	Configure the Flap Guard function.
	Configure the Loop Guard function.
	Configure the Root Guard function.
	Configure the TC protection function.

27.2.1 Configure Basic Functions of an STP *-B -S -E -A*

Configuration Conditions

None

Enable the STP Function

After the STP function is enabled, devices start to run the STP protocol. The devices exchange BPDU packets to form a stable tree network topology, and network loops are eliminated.

Table 27-2 Enabling the STP Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enabling the STP function globally.	**spanning-tree enable**	Mandatory.

Step	Command	Description
		By default, the STP function is disabled globally.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Enabling the STP function on a port.	**spanning-tree enable**	Optional. By default, the STP function is enabled on a port.

Configure MST Regions

Dividing an entire network into multiple MST regions helps to shorten the network convergence time. VLAN packets are transmitted through the corresponding MST Instances in MST regions and transmitted through CSTs between MST regions.

Table 27-3 Configuring MST Regions

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the MST region configuration mode.	**spanning-tree mst configuration**	-
Configure an MST region name.	**region-name** *region-name*	Mandatory. By default, the name of an MST region is the MAC address of the local device.

Step	Command	Description
Configure the MSTP revision level.	**revision-level** *revision-level*	Mandatory. By default, the MSTP revision level is 0.
Configure a VLAN mapping table.	**instance** *instance-id* **vlan** *vlan-list*	Mandatory. By default, all VLANs are mapped to instance 0.
Activate MST region parameter configuration.	**active configuration pending**	Mandatory. By default, MST region parameters do not take effect immediately after modification.

NOTE

- MST region parameters do not take effect immediately after they are modified. Instead, you need to run the **active configuration pending** command to activate the parameters and trigger re-calculation of the STP. To cancel MST region parameter configuration, use the **abort configuration pending** command.

27.2.2 Configure Bridge Properties *-B -S -E -A*

Configuration Conditions

None

Configure the Priority of a Bridge

The bridge priority and MAC address form the bridge ID. A smaller ID indicates a higher priority. The bridge with the highest priority is elected as the root bridge. One device may have different bridge priority in different STP instances.

Table 27-4 Configuring the Priority of a Bridge

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Configure the priority of a bridge.	**spanning-tree mst instance** *instance-id* **priority** *priority-value*	Mandatory. By default, the priority of the bridge in all STP instances is 32768.

NOTE

- The step of bridge priorities is 4096, that is, the valid values include: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28673, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

Configure Hello Time

After the network topology becomes stable, the root bridge sends BPDU packets at the interval of Hello Time to inform other bridges of its role as the root bridge so that the other bridges can recognize its role. The designated bridge maintains the existing STP topology according to the BPDU packet, and it forwards the BPDU packet to other devices. If the designated bridge does not receive BPDU packets at a period of time as long is three times Hello Time, it regards the link as faulty. In this way, the STP re-calculates the network topology to obtain a new active path, ensuring the network connectivity.

Table 27-5 Configuring Hello Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Hello Time.	**spanning-tree mst hello-time** *seconds*	Mandatory. By default, Hello Time is 2 seconds.

NOTE

- Forward Delay, Hello Time, and Max Age must meet the following requirement; otherwise, frequent network flapping may be cause.

  2 × (Forward_Delay – 1.0seconds) ≥ Max_Age

  Max_Age ≥ 2 × (Hello_Time + 1.0seconds)

Configure Forward Delay

In STP, when the root port or designated port migrates from the Discarding status to the Forwarding status, the topology change cannot be learned by the entire network immediately. To prevent temporary loops, the port migrates to the Learning status in the first Forward Delay, and then waits another Forward Delay to migrate to the Forwarding status.

Table 27-6 Configuring Forward Delay

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Forward Delay.	**spanning-tree mst forward-time** *seconds*	Mandatory. By default, Forward Delay is 15 seconds.

Configure Max Age

Max Age refers to the life cycle of BPDU configuration messages while they are broadcast in a network. When a configuration message is transmitted crossing regions, after it passes through an MST region, one is added to Message Age in the configuration message. If the device receives a configuration message and finds that the value of Message Age in the configuration message is larger than the value of Max Age, the device discards the configuration message, and the configuration message is no longer used in STP calculation.

Table 27-7 Configuring Max Age

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Max Age.	**spanning-tree mst max-age** *seconds*	Mandatory. By default, Max Age is 20 seconds.

Configure the Maximum Number of Hops in an MST Region

You can limit the size of an MST region by configuring the maximum number of hops in the MST region. A larger number of hops in an MST region mean a larger MST region. In one MST region, starting from the region root, once the configuration message is forwarded by a device, the number of hops is decreased by one. If the number of hops of a configuration message is 0, the device discards the configuration message. Therefore, the device which is beyond the maximum number of hops cannot participate in STP calculation in the region.

Table 27-8 Configuring the Maximum Number of Hops in an MST Region

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the maximum number of hops in an MST region.	**spanning-tree mst max-hops** *max-hops-value*	Mandatory. By default, the maximum number of hops in an MST region is 20.

27.2.3 Configure STP Port Properties *-B -S -E -A*

Configuration Conditions

None

Configure the Priority of a Port

A port ID consists of port priority and port index. Port ID affects election of the port role. A smaller port ID indicates a higher priority. One port may have different port priority in different STP instances.

Table 27-9 Configuring the Priority of a Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configuring the priority of a port.	**spanning-tree mst instance** *instance-id* **port-priority** *priority-value*	Mandatory. By default, the priority of the port in all STP instances is 128.

NOTE

- The step of port priorities is 16, that is, the valid values include: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240.

Configure the Default Path Cost Standard for a Port

Compared with the path cost calculated based on the IEEE 802.1D-1998 standard, the path cost calculated based on the IEEE 802.1T-2001 is larger. With the increase of the link rate, the path cost value quickly decreases.

Table 27-10 Configuring the Default Path Cost Standard for a Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the default path cost standard for a port.	s**panning-tree pathcost method** { **dot1D-1998 | dot1T-2001** }	Mandatory. By default, the IEEE 802.1T-2001 standard is used to calculate the default path cost of the port.

Configure the Path Cost of a Port

The port path cost affects election of the port role. A smaller port path cost means a better link. One port may have different port path cost in different STP instances.

Table 27-11 Configuring the Path Cost of a Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the path cost of a port.	**spanning-tree mst instance** *instance-id* **cost** *cost-value*	Mandatory. By default, the path cost is automatically calculated according to the port rate.

Configure the Maximum Transmitting Rate of BPDU Packets

The maximum transmitting rate of BPDU packets limits the number of BPDU packets that can be transmitted during the Hello Time of a device. This prevents the device from sending too many BPDU packets which may cause frequent STP calculation for other devices.

Table 27-12 Configuring the Maximum Transmitting Rate of BPDU Packets

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the maximum transmitting rate of BPDU packets.	**spanning-tree transmit hold-count** *hold-count-number*	By default, a port can send a maximum of 6 BPDU packets within Hello Time.

Configure Timeout Factor of BPDU Packets

In a stable network topology, designated port will send a BPDU packet to neighbored device every HELLO TIME. Usually if the device doesn't receive the BPDU packet from upper devices three times beyond HELLO TIME, it is considered that the network topology changes, which will start an STP re-election.

However in a stable network topology, if the upper device can’t receive the BPDU packet in the case of busy or any other reason, it will start an STP re-election. In this case, you can configure the timeout factor to avoid such calculation.

Table 27-13 Configure the Timeout Factor of BPDU Packets

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure time factor of BPDU packets	**spanning-tree timer-facor ho** *times-number*	By default, if the device doesn't receive the BPDU packet from upper devices three times beyond HELLO TIME, it is considered that the network topology changes, which will start an STP re-election. In stacking environment, it is recommended to configure the timeout factor as 6.

Configure an Edge Port

Edge ports are the ports that are directly connected to user terminals. If an edge port is UP/DOWN, it does not cause temporary loops. Therefore, an edge port can quickly migrate from the Discarding status to the Forwarding status without delay time. In addition, if an edge port is UP/DOWN, it does not send TC BPDUs. This prevents unnecessary STP re-calculation.

If an edge port receives BPDU packets, it becomes a non-edge port again. Then, the port can become the edge port again only after it is reset.

Table 27-14 Configuring Edge Ports

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure an edge port.	**spanning-tree portfast edgeport**	Mandatory. By default, a port is a not an edge port.

Configure the Port Link Type

If two devices are directly connected, you can configure the port link type to point-to-point link. The ports of the point-to-point link type can quickly migrate from the Discarding status to the Forwarding status without delay time.

Table 27-15 Configuring the Port Link Type

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the port link type.	**spanning-tree link-type** { **point-to-point | shared** }	Mandatory. By default, the port link type is set according to the port duplex mode. If the port works in the full duplex mode, the port is set to the point-to-point link type. If the port works in the half

Step	Command	Description
		duplex mode, the port is set to the shared link type.

27.2.4 Configure the Working Mode of an STP *-B -S -E -A*

The working mode of an STP determines the mode in which devices run and determines the encapsulation format of BPDU packets that are sent out. If a port that works in the MSTP mode is found to be connected to a device that runs RSTP, the port automatically migrates to the RSTP mode. If a port that works in the MSTP mode or MSTP mode is found to be connected to a device that runs STP, the port automatically migrates to the STP compatible mode.

Configuration Conditions

None

Configure the Working Mode of an STP

Table 27-16 Configuring the Working Mode of an STP

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the working mode of an STP.	**spanning-tree mode** { **stp** | **rstp** | **mstp** }	Mandatory. By default, the working mode of an STP is MSTP.

27.2.5 Configure the STP Protection Function *-B -S -E -A*

Configuration Conditions

None

Configure the BPDU Guard Function

For an access layer device, the access port is usually directly connected to the user terminal or file server. At this time, the port is set to the edge port to realize fast migration of port statuses. When an edge port receives BPDU packets, it automatically changes to a non-edge port to cause re-generation of the STP. Normally, an edge port does not receive BPDU packets. However, if someone sends faked BPDU packets to attack the device in a malicious manner, network flapping may be caused. The BPDU Guard function is used to prevent such attacks. If an edge port on which the BPDU Guard function is enabled receives BPDU packets, the port is closed.

Table 27-17 Configuring the BPDU Guard Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the BPDU Guard function.	**spanning-tree bpdu guard**	Mandatory. By default, the BPDU Guard function is disabled on the port.

Configure the BPDU Filter Function

After the BPDU Filter function is enabled on an edge port, the port does not send or receive BPDU packets.

Table 27-18 Configuring the BPDU Filter Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		takes effect only within the aggregation group.
Configure the BPDU Filter function.	**spanning-tree bpdu filter**	Mandatory. By default, the BPDU Filter function is disabled.

Configure the Flap Guard Function

In a stable topology environment, the root port is usually not changed. However, if the links in the network are not stable or the network experiences attacks with external BPDU packets, frequent switchover of root ports may be caused, and finally network flapping is caused.

The Flap Guard function prevent frequent switchover of root ports. After the Flap Guard function is enabled, if the root port role change frequency of an STP instance exceeds the specified threshold, the root port of the instance enters the Flap Guard status. In this case, the root port is always in the Discarding status, and it starts normal STP calculation only after the recovery time times out.

Table 27-19 Configuring the Flap Guard Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the Flap Guard function.	**spanning-tree flap-guard enable**	Mandatory. By default, the Flap Guard function is disabled.
Configure the maximum number of root port changes that are allowed within a detection period.	**spanning-tree flap-guard max-flaps** *max-flaps-number* **time** *seconds*	Optional. By default, after the Flap Guard function is enabled, if five root port role changes occurs for an instance within 10 seconds, the port enters the Flap Guard status.
Configure the Flap Guard recovery time.	**spanning-tree flap-guard max-flaps** *count* **time** *seconds*	Optional. By default, the Flap Guard recovery time is 30 seconds.

Configure the Loop Guard Function

The local device maintains the statuses of the root port and other blocked ports according to the BPDU packets that are periodically sent by the upstream device. In the case of link congestion or unidirectional link failure, the ports fail to receive BPDU packets from the upstream device, the STP message on the port times out. Then, the downstream devices re-elect port roles. The downstream device ports that fail to receive BPDU packets change to designated port, while blocked ports migrate to the Forwarding status, resulting in loops in the switching network.

The Loop Guard function can restrain generation of such loops. After the Loop Guard function is enabled on a port, if the port times out owing to the failure to receive BPDU packets from the upstream device, in re-calculating the port role, the port is set to the Discarding status, and the port does not participate in STP calculation. If an instance on the port receives BPDU packets again, the port participates in STP calculation again.

Table 27-20 Configuring the Loop Guard Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the Loop Guard function.	**spanning-tree guard** { **loop** | **root** | **none** }	Mandatory. By default, the Loop Guard function is disabled on the port.

NOTE

- On a port, either the Root Guard function or the Loop Guard function can be enabled at a time.

Configure the Root Guard Function

The root bridge and backup root bridge of an STP must be in the same region, especially the CIST root bridge and its backup bridge. In network design, usually the CIST root bridge and its backup bridge are placed in the core region with high bandwidth. However, owning to incorrect configuration or malicious attacks in the network, the legal root bridge in the network may receive a BPDU packet with a higher priority. In this way, the current legal bridge may lose its role as the root bridge, and improper change of the network topology is caused. The illegal change may lead the traffic that should be transmitted through a high-speed link to a low-speed link, causing network congestion.

The Root Guard function prevents occurrence of such case. If the Root Guard function is enabled on a port, the port can only act as the designated port in all instances. If the port receives a better BPDU configuration message, the port is set to the Discarding status. If it does not receive better BPDU configuration message in a period of time, the port resumes its previous status. It is recommended that you enable the Root Guard function on the specified port of the root bridge.

Table 27-21 Configuring the Root Guard Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure the Root Guard function.	**spanning-tree guard** { **loop** | **root** | **none** }	Mandatory. By default, the Root Guard function is disabled on the port.

NOTE

- On a port, either the Root Guard function or the Loop Guard function can be enabled at a time.

Configure the TC Protection Function

If the network topology changes, to ensure normal forwarding of service data during the topology change process, when devices handle TC packets, they will refresh the MAC addresses. Attacks with faked TC packets may cause the devices to refresh MAC addresses frequently. This affects calculation of the STP and leads to a high CPU occupancy.

The TC protection function prevents occurrence of such case. After the TC protection function is enabled, once a TC packet is received within the TC protection interval, the TC counter counts one. If the TC counter is equal to or larger than the threshold, it enters a suppressed status. Then, the devices do not refresh MAC addresses in handling later TC packets. After the TC protection interval, the suppressed status is changed to the normal status, and the TC counter is cleared and started again.

Table 27-22 Configuring the TC Protection Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the TC protection function.	**spanning-tree tc-protection enable**	Optional. By default, the TC protection function is enabled.
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure a TC protection interval.	**spanning-tree tc-protection interval** *seconds*	Mandatory. By default, the TC protection interval is 2 seconds.
Configure the TC protection threshold.	**spanning-tree tc-protection threshold** *threshold-value*	Mandatory. By default, the TC protection threshold is 3.

27.2.6 STP Monitoring and Maintaining *-B -S -E -A*

Table 27-23 STP Monitoring and Maintaining

Command	**Description**
clear spanning-tree detected-protocols	Perform the mCheck operation globally or on a specified port.
show spanning-tree mst [**configuration** [**current** | **pending**] | **detail** | **instance** *instance-id* [**detail**] | { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* } [**instance** *instance-id*]]	Displays the configuration and status information about the STP.
show configuration { current | pending }	Displays the configuration of MST regions.

27.3 STP Typical Configuration Example

27.3.1 MSTP Typical Application *-B -S -E -A*

Network Requirements

- Four devices in the network are in the same MST domain. Device1 and Device2 convergence layer devices, while Device3 and Device4 are access layer devices.
- To reasonably balance traffic on the links to realize load sharing and redundancy backup, configure packets of VLAN2 to be forwarded following instance 1. The root bridge of instance 1 is Device1. Packets of VLAN3 are forwarded following instance 2. The root bridge of instance 2 is Device2. Packets of VLAN4 are forwarded following instance 0.

Network Topology

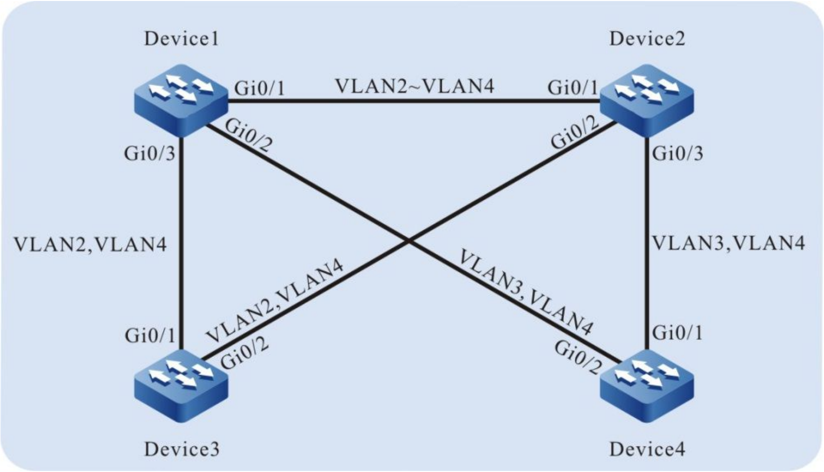


Figure 27-1 Networking for MSTP Typical Application

Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Device1, create VLAN2-VLAN4, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN2-VLAN4 to pass.

```
Device1(config)#vlan 2-4
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-4
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN3 and VLAN4 to pass. Configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN2 and VLAN4 to pass. (Omitted)

#On Device2, create VLAN2-VLAN4. Configure the link type of ports gigabitethernet0/1-gigabitethernet0/3 to Trunk, configure gigabitethernet0/1 to allow services of VLAN2-VLAN4 to pass, gigabitethernet0/2 to allow services of VLAN2 and VLAN4 to pass, and gigabitethernet0/3 to allow services of VLAN3 and VLAN4 to pass. (Omitted)

#On Device3, create VLAN2-VLAN4, configure the link type of port gigabitethernet0/1-gigabitethernet0/2 to Trunk and allow services of VLAN2-VLAN4 to pass. (Omitted)

#On Device4, create VLAN3 and VLAN4, configure the link type of port gigabitethernet0/1-gigabitethernet0/2 to Trunk and allow services of VLAN3 and VLAN4 to pass. (Omitted)

Step 2: Configure an MST region.

#On Device1, configure an MST region. Set the domain name to admin, the revision level to 1, map instance 1 to VLAN2, map instance 2 to VLAN3, and activate the MST region.

```
Device1#configure terminal
Device1(config)#spanning-tree mst configuration
Device1(config-mst)#region-name admin
Device1(config-mst)#revision-level 1
Device1(config-mst)#instance 1 vlan 2
Device1(config-mst)#instance 2 vlan 3
Device1(config-mst)#active configuration pending
Device1(config-mst)#exit
```

NOTE

- The MST region configuration of Device2, Device3, and Device 4 is far different from that of Device1. (Omitted)

#On Device1, configure the priority of MST Instance 1 to 0. On Device2, configure the priority of MST Instance 2 to 0.

```
Device1(config)#spanning-tree mst instance 1 priority 0
Device2(config)#spanning-tree mst instance 2 priority 0
```

#On Device1, enable the STP globally.

```
Device1(config)#spanning-tree enable
```

NOTE

- The configuration for enabling the STP globally on Device2, Device3, and Device 4 is far different from that on Device1. (Omitted)

Step 3: Check the result.

#After the network topology is stable, check the calculation result of all STP instances.

```
Device1#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped: 1,4-4094
 Bridge              address 0000.0000.008b priority 32768
 Region root          address 0000.0000.008b priority 32768
   Designated root       address 0000.0000.008b priority 32768
                       root: 0, rpc: 0, epc: 0, hop: 20
 Operational  hello time 2, forward time 15, max age 20
 Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 6
 Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Configured timer factor: 3
 Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1               Desg  FWD    20000   128.001 P2P
gi0/2               Desg  FWD    20000   128.002 P2P
gi0/3               Desg  FWD    20000   128.003 P2P
MST Instance 01        vlans mapped: 2
 Bridge ID           address 0000.0000.008b priority 1/0
 Designated root       address 0000.0000.008b priority 1
                       root: 0, rpc: 0, hop: 20
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1               Desg  FWD    20000   128.001 P2P
gi0/3               Desg  FWD    20000   128.003 P2P
MST Instance 02        vlans mapped: 3
 Bridge ID           address 0000.0000.008b priority 32770/32768
 Designated root       address 94ae.e354.5c96 priority 2
                       root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1               Root  FWD   20000   128.001 P2P
gi0/2               Desg  FWD    20000   128.002 P2P
```

#On Device2, query the calculation result of all STP instances. According to the result, port gigabitethernet0/2 of Device2 is blocked in both instance 0 and instance 1.

```
Device2#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Mode MSTP
MST Instance 00        vlans mapped:  1,4-4094
 Bridge              address 94ae.e354.5c96 priority 32768
 Region root          address 0000.0000.008b priority 32768
   Designated root       address 0000.0000.008b priority 32768
                       root: 32769, rpc: 20000, epc: 0, hop: 19
 Operational  hello time 2, forward time 15, max age 20
 Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 6
 Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Configured timer factor: 3
 Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
```

```
-------------------- ----- ---- --------- --------- --------------------------
gi0/1                Root  FWD     20000   128.001 P2P
gi0/2                Alte  DIS     20000   128.002 P2P
gi0/3                Desg  FWD     20000   128.003 P2P
MST Instance 01         vlans mapped:  2
 Bridge ID            address 94ae.e354.5c96 priority 32769/32768
 Designated root       address 0000.0000.008b priority 1
                       root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1                Root  FWD     20000   128.001 P2P
gi0/2                Alte  DIS     20000   128.002 P2P
MST Instance 02         vlans mapped:  3
 Bridge ID            address 94ae.e354.5c96 priority 2/0
 Designated root       address 94ae.e354.5c96 priority 2
                       root: 0, rpc: 0, hop: 20
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1                Desg  FWD     20000   128.001 P2P
gi0/3                Desg  FWD     20000   128.003 P2P
```

#On Device3, query the calculation result of all STP instances.

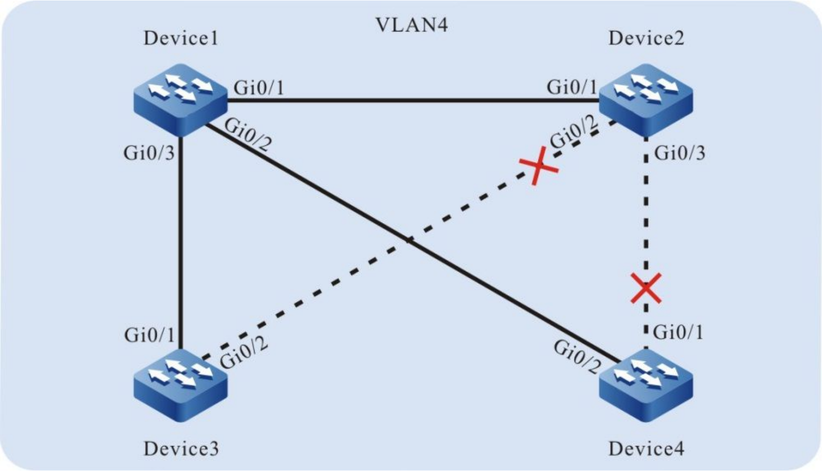
```
Device3#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00         vlans mapped: 1,4-4094
 Bridge               address 0000.0305.070a priority 32768
 Region root           address 0000.0000.008b priority 32768
   Designated root       address 0000.0000.008b priority 32768
                       root: 32769, rpc: 20000, epc: 0, hop: 19
 Operational  hello time 2, forward time 15, max age 20
 Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 6
 Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Configured timer factor: 3
 Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1                Root  FWD     20000   128.001 P2P
gi0/2                Desg  FWD     20000   128.002 P2P
MST Instance 01         vlans mapped: 2
 Bridge ID            address 0000.0305.070a priority 32769/32768
 Designated root       address 0000.0000.008b priority 1
                       root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1                Root  FWD     20000   128.001 P2P
gi0/2                Desg  FWD     20000   128.002 P2P
```

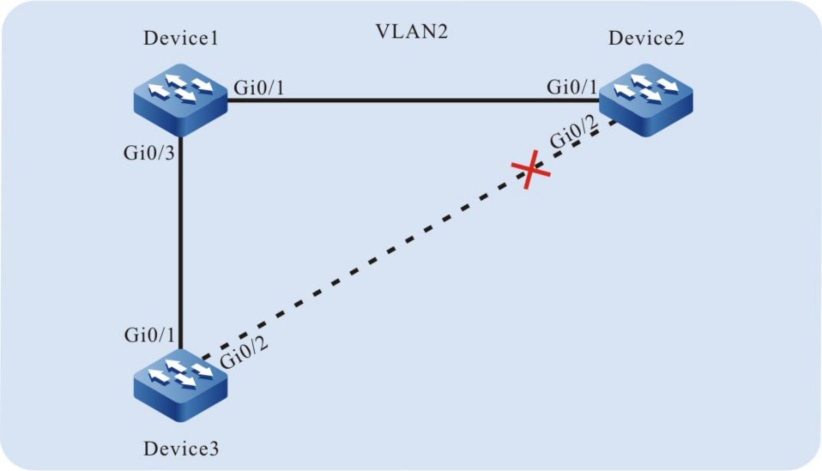
#On Device4, query the calculation result of all STP instances. According to the result, port gigabitethernet0/1 of Device4 is blocked in instance 0, and port gigabitethernet0/2 is blocked in instance 2.

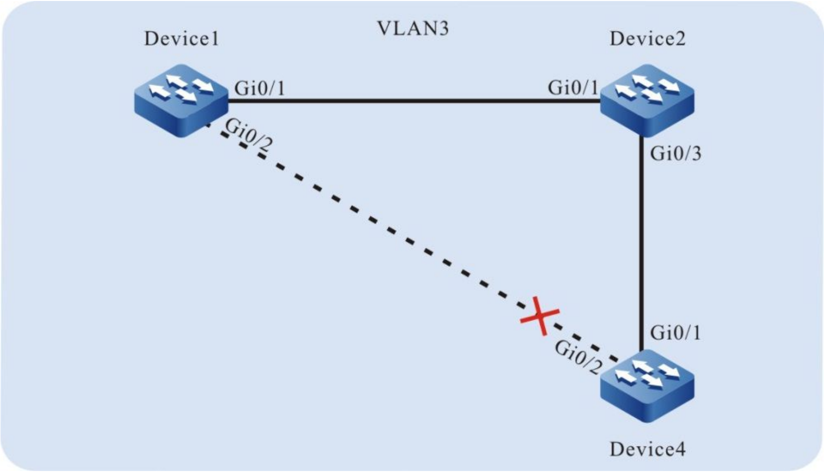
```
Device4#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00         vlans mapped:  1,4-4094
 Bridge               address 94ae.e358.dc0c priority 32768
 Region root           address 0000.0000.008b priority 32768
   Designated root       address 0000.0000.008b priority 32768
                       root: 32769, rpc: 20000, epc: 0, hop: 19
 Operational  hello time 2, forward time 15, max age 20
 Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 6
 Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
 Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
          Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1                Alte  DIS     20000   128.001 P2P
```

```
gi0/2              Root  FWD     20000    128.002 P2P
MST Instance 02         vlans mapped:  3
 Bridge ID            address 94ae.e358.dc0c priority 32770/32768
 Designated root       address 94ae.e354.5c96 priority 2
                    root: 32769, rpc: 20000, hop: 19
Configured timer factor: 3
Topology Change Count:4, last change occured:0 hour 1 minute 0 second(60 seconds)
         Interface  Role  Sts      Cost  Prio.Nbr Type
-------------------- ----- ---- --------- --------- --------------------------
gi0/1              Root  FWD    20000    128.001 P2P
gi0/2              Alte  DIS    20000    128.002 P2P
```

Based on the STP calculation result of the four devices, the tree diagrams corresponding to MST Instance 0 (mapped to VLAN4), MST Instance 1 (mapped to VLAN2), and MST Instance 2 (mapped to VLAN3) are obtained.






VLAN3
Device1
Device2
Gi0/1
Gi0/1
Gi0/2
Gi0/3
Gi0/1
Gi0/2
Device4

28 Loopback Detection

28.1 Overview

In the Ethernet, if the destination of some packet fails to be recognized, they will be flooded in a VLAN. If a loop exists in the network, the packets circulate and multiply without limit, and finally they will use up the bandwidth. Then, the network fails to provide normal communication.

There are two types of loops, loop between different ports of a device, and loop on one port of a device. The two types of loops can be detected through loopback detection.

After the loopback detection function is enabled, a port sends loopback detection packets at intervals in the VLAN to which it has been added to check whether a loop exists in the network. When a port receives a loopback detection packet that the local device sent, it determines that a loop exists in the network. Then, the port is disabled to prevent the local loop from affecting the entire network.

28.2 Loopback Detection Function Configuration

Table 28-1 Loopback Detection Function List

Configuration Tasks	
Configure basic functions of loopback detection.	Enable the global loopback detection control switch.
	Enable the loopback detection control switch of a port or aggregation group.
Configure basic parameters of loopback detection.	Configure the interval at which loopback detection packets are sent.
	Configure the Error-Disable action on a port.

28.2.1 Configure Basic Functions of Loopback Detection *-B -S -E -A*

Configuration Conditions

None

Enable the Global Loopback Detection Control Switch

The global loopback detection control switch is used to enable the global loopback detection function. The loopback detection configuration of a port takes effect only after the global loopback detection control switch is enabled.

Table 28-2 Enabling the Global Loopback Detection Control Switch

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the global loopback detection control switch.	**loopback-detection enable**	Mandatory. By default, the global loopback detection control switch is disabled.

Enable the Loopback Detection Control Switch of a Port or Aggregation Group

After the loopback detection function is enabled, a port sends loopback detection packets at intervals in the VLAN to which it has been added to check whether a loop exists in the network.

Table 28-3 Enabling the Loopback Detection Control Switch of a Port or Aggregation Group

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		subsequent configuration takes effect only within the aggregation group.
Enable the loopback detection control switch of a port or aggregation group.	**loopback-detection enable**	Mandatory. By default, the loopback detection control switch of a port or aggregation group is disabled.

NOTE

- In loopback detection configuration task, you must enable the global loopback detection control switch before the loopback detection configuration on a port takes effect.

28.2.2 Configure Basic Parameters of Loopback Detection *-B -S -E -A*

Configuration Conditions

None

Configure the Interval at Which Loopback Detection Packets Are Sent

In a loopback detection, loopback detection packets are sent periodically to detect loops in the network. You can modify the interval at which loopback detection packets are sent according to the actual network requirement.

Table 28-4 Configuring the Interval at Which Loopback Detection Packets Are Sent

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface configuration mode.	**interface** *interface-name*	At least one option must be selected.

Step	Command	Description
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure the interval at which loopback detection packets are sent.	**loopback-detection enable interval-time** *interval-time-value*	Mandatory. By default, the interval at which loopback detection packets are sent is 30 seconds.

Configure the Error-Disable Action on a Port

If a port allows the Error-Disable action, the port is controlled. After a port detects a loop, it performs the Error-Disable action to close the port so as to eliminate the loop. If the port is not in the controlled status, the port only prints loop prompt message instead of closing the port. In this case, the loop has not been eliminated.

Table 28-5 Configuring the Error-Disable Action on a Port

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 Ethernet interface	**interface** *interface-name*	

Step	Command	Description
configuration mode.		At least one option must be selected. After you enter the layer-2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Enter the aggregation group configuration mode.	**link-aggregation** *link-aggregation-id*	
Configure whether the port allows the Error-Disable function.	**loopback-detection enable control**	Mandatory. By default, after a port detects a loop, it performs the Error-Disable action.

28.2.3 Loopback Detection Monitoring and Maintaining *-B -S -E -A*

Table 28-6 Loopback Detection Monitoring and Maintaining

Command	Description
show loopback-detection [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Displays the configuration information of all ports or a specified port in loopback detection.

28.3 Typical Configuration Example of Loopback Detection

28.3.1 Configure Remote Loopback Detection *-B -S -E -A*

Network Requirements

- Device1 and Device2 are directly connected, and Device2 has two ports which form a self-loop.
- On Device1, loopback detection has been enabled.
- After Device1 detects a loop, it closes the interconnected port to eliminate the loop.

Network Topology

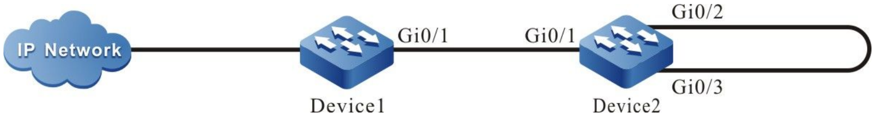


Figure 28-1 Networking for Configuring the Remote Loopback Detection Function

Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Device1, create VLAN2.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#On Device1, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device2, create VLAN2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device2, configure the link type of port gigabitethernet0/1 to Trunk and configure the port to allow services of VLAN2 to pass. Configure the link type of ports gigabitethernet0/2 and gigabitethernet0/3 to access and configure the ports to allow services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

Step 2: Enable the loopback detection function.

#On Device1, enable the loopback detection function globally.

```
Device1(config)#loopback-detection enable
```

#On port gigabitethernet0/1 of Device1, enable the loopback detection function.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, query the loopback detection status.

```
Before a loop is detected:
Device1#show loopback-detection
 ------------------------------------------------------------
 Global loopback-detection : ENABLE
 -------------------  --------  ------- ------------  -------
 Interface            Loopback  Time(s) State        Control
 -------------------  --------  ------- ------------  -------
 gi0/1              ENABLE    30     NORMAL        TRUE
 gi0/2              DISABLE   30     NORMAL        TRUE
```

Step 3: Check the result.

#On Device1, query the loopback detection status.

```
After a loop is detected:
Device1#show loopback-detection
 ------------------------------------------------------------
 Global loopback-detection : ENABLE
 -------------------  --------  ------- ------------  -------
 Interface            Loopback  Time(s) State        Control
 -------------------  --------  ------- ------------  -------
 gi0/1              ENABLE    30     ERR-DISABLE   TRUE
 gi0/2              DISABLE   30     NORMAL        TRUE
```

#A loop has been detected on Device1. The port gigabitethernet0/1 is to be closed, and the device outputs the following prompt information:

```
Jan   3 03:30:30: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet0/1,
detected in vlan2 from gigabitethernet0/1
Jan  3 03:30:30: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Jan  3 03:30:30: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
```

#On Device1, query the status of port gigabitethernet0/1, and you will find that the status of the port is changed to Down.

```
Device1#show interface gigabitethernet 0/1
gigabitethernet0/1 configuration information
       Description      :
       Status           : Enabled
       Link             : Down  (Err-disabled)
       Set Speed        : Auto
       Act Speed        : Unknown
       Set Duplex       : Auto
       Act Duplex       : Unknown
       Set Flow Control : Off
       Act Flow Control : Off
       Mdix             : Auto
       Mtu              : 1824
       Port mode        : LAN
       Port ability     : 10M HD,10M FD,100M HD,100M FD,1000M FD
       Link Delay       : No Delay
       Storm Control    : Unicast Disabled
       Storm Control    : Broadcast Disabled
       Storm Control    : Multicast Disabled
       Storm Action     : None
Port Type        : Nni
```

```
Pvid            : 1
Set Medium       : Copper
Act Medium       : Copper
                Mac Address      : 0000.0000.008b
```

28.3.2 Configure Local Loopback Detection *-B -S -E -A*

Network Requirements

- Device1 and Device2 form a loop through two links, and all the ports in the loop is in one VLAN.
- On Device1, loopback detection has been enabled.
- After Device1 detects a loop, it closes the interconnected port to eliminate the loop.

Network Topology

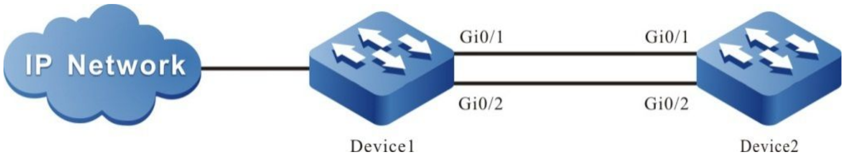


Figure 28-2 Networking for Configuring the Local Loopback Detection Function

Configuration Steps

Step 1: Configure VLANs, and configure the link type of the ports.

#On Device1, create VLAN2.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#On Device1, configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 to Trunk and allow services of VLAN2 to pass.

```
Device1(config)# interface gigabitethernet 0/1-0/2
Device1(config-if-range)#switchport mode trunk
Device1(config-if-range)#switchport trunk allowed vlan add 2
Device1(config-if-range)#exit
```

#On Device2, create VLAN2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 to Trunk and allow services of VLAN2 to pass.

```
Device2(config)# interface gigabitethernet 0/1-0/2
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#exit
```

Step 2: Enable the loopback detection function.

#On Device1, enable the loopback detection function globally.

```
Device1(config)#loopback-detection enable
```

#On port gigabitethernet0/1 of Device1, enable the loopback detection function.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, query the loopback detection status.

```
Before a loop is detected:
Device1#show loopback-detection
 ------------------------------------------------------------
 Global loopback-detection : ENABLE
 -------------------  --------  ------- ------------  -------
 Interface            Loopback  Time(s) State        Control
 -------------------  --------  ------- ------------  -------
 gi0/1              ENABLE    30     NORMAL        TRUE
 gi0/2              DISABLE   30     NORMAL        TRUE
```

Step 3: Check the result.

#On Device1, query the loopback detection status.

```
After a loop is detected:
Device1#show loopback-detection
 ------------------------------------------------------------
 Global loopback-detection : ENABLE
 -------------------  --------  ------- ------------  -------
 Interface            Loopback  Time(s) State        Control
 -------------------  --------  ------- ------------  -------
 gi0/1              ENABLE    30     ERR-DISABLE   TRUE
 gi0/2              DISABLE   30     NORMAL        TRUE
```

#A loop has been detected on Device1. The port gigabitethernet0/1 is to be closed, and the device outputs the following prompt information:

```
Jan  3 03:29:59: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet0/1,
detected in vlan2 from gigabitethernet0/2
Jan  3 03:29:59: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Jan  3 03:29:59: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
```

#On Device1, query the status of port gigabitethernet0/1, and you will find that the status of the port is changed to Down.

```
Device1#show interface gigabitethernet 0/1
gigabitethernet0/1 configuration information
     Description      :
     Status           : Enabled
     Link             : Down  (Err-disabled)
     Set Speed        : Auto
     Act Speed        : Unknown
     Set Duplex       : Auto
     Act Duplex       : Unknown
     Set Flow Control : Off
     Act Flow Control : Off
     Mdix             : Auto
     Mtu              : 1824
     Port mode        : LAN
     Port ability     : 10M HD,10M FD,100M HD,100M FD,1000M FD
     Link Delay       : No Delay
     Storm Control    : Unicast Disabled
     Storm Control    : Broadcast Disabled
     Storm Control    : Multicast Disabled
     Storm Action     : None
```

```
Port Type        : Nni
        Pvid            : 1
        Set Medium       : Copper
        Act Medium       : Copper
 Mac Address      : 0000.0000.008b
```

29 Error-Disable Management

29.1 Overview

The Error-Disable function is an error detection and fault recovery mechanism on ports.

Exceptions on ports may degrade the performance of the entire network or bring down the entire network. The Error-Disable function can limit the abnormality within a single device or part of the network, preventing the abnormality from affecting other normal ports and preventing the abnormality from spreading.

If an exception is detected on an open port, the port is automatically closed so that the port will not forward packets. That is, if an error condition is triggered on the port, the port is automatically disabled. This is the Error-Disable management function, and the port status is the Error-Disabled status.

Currently, the following functions are supported: storm suppression, port security, link flapping, DHCP rate limit, BPDU Guard, ARP detection, L2 protocol tunnel, loopback detection, OAM, and Monitor Link.

If an exception is detected on a port through the above functions, the port is automatically closed, and it is set to the Error-Disabled status. However, this status cannot continue. After the fault is eliminated, the port needs to be enabled again, and the Error-Disabled status of the port needs to be cleared so that the port can continue to forward packets. Here the automatic recovery mechanism of the Error-Disable management function is involved.

29.2 Error-Disable Management Function Configuration

Table 29-1 Error-Disable Management Function List

Configuration Tasks	
Configure Error-Disable basic functions.	Configure Error-Disable error detection.
Configure Error-Disable automatic recovery.	Configure Error-Disable automatic recovery.
	Configure the interval for Error-Disable automatic discovery.

29.2.1 Configure Error-Disable Basic Functions *-B -S -E -A*

Configuration Conditions

None

Configure Error-Disable Error Detection

After the Error-Disable detection of the specification function is configured, if an exception is detected on the port, the system automatically close the port and set the port to the Error-Disabled status.

Table 29-2 Configuring Error-Disable Error Detection

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Error-Disable error detection.	**errdisable detect cause** { **all** | **bpduguard** | **dai** | **dhcp-snooping** | **l2pt** | **oam** | **storm-control** | **link-flap** | **port-security** | **loopback-detect** | **monitor-link** }	Mandatory. By default, it is allowed that all the listed functions close a port and set the port to the Error-Disabled status.

29.2.2 Configure Error-Disable Automatic Recovery *-B -S -E -A*

Configure Error-Disable Automatic Recovery

The Error-Disable error detection mechanism enables specified functions to close a port. To quickly recover the port so that it can continue to forward packets, an automatic recovery mechanism is provided. With the mechanism, the port is automatically re-enabled after a specified interval.

Table 29-3 Configuring Error-Disable Automatic Recovery

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure Error-Disable automatic recovery.	**errdisable recovery cause** { **all** | **bpduguard** | **dai** | **dhcp-snooping** | **eips-udld** | **l2pt** | **link-flap** | **loopback-detect** | **oam** | **port-security** | **storm-control** | **ulfd** }	Mandatory. By default, a port cannot be automatically enabled, and the Error-Disabled status set by the listed functions cannot be automatically cleared. However, by default, a port can be automatically enabled and the Error-Disabled status can be automatically cleared if its status is set by the Link-Flap function.

Configure the Interval for Error-Disable Automatic Discovery

You can configure the interval for a port to automatically recover normal after it port is closed by the Error-Disable error detection mechanism.

Table 29-4 Configuring the Interval for Error-Disable Automatic Discovery

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the interval for Error-Disable automatic discovery.	**errdisable recovery interval** *interval-value*	Mandatory. By default, the interval at which a port is enabled and its Error-Disabled status is cleared is 300 seconds.

29.2.3 Error-Disable Management Monitoring and Maintaining *-B -S -E -A*

Table 29-5 Error-Disable Management Monitoring and Maintaining

Command	Description
show errdisable detect	Displays whether it is allowed that all the listed functions close a port and set the port to the Error-Disabled status.
show errdisable recovery	Displays whether a port can be automatically enabled, and whether the Error-Disabled status set by the listed functions can be cleared automatically.
show { **interface** *interface-list* | **link-aggregation** *link-aggregation-id* } **status err-disabled**	Displays the information about Error-Disabled status setting of a specified port or aggregation group.

29.3 Typical Configuration Example of Error-Disable Management

29.3.1 Combination of Error-Disable and Storm Suppression *-B -S -E -A*

Network Requirements

- PC accesses IP Network through Device. On Device, the storm suppression and Error-Disable functions have been enabled.
- If a port of a device receives a large number of broadcast packets and then disabled, Error-Disable can re-enable the port according to the policy.

Network Topology

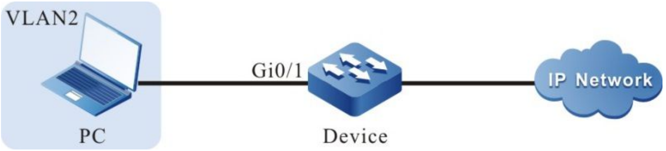


Figure 29-1 Networking for Combination of Error-Disable and Storm Suppression

Configuration Steps

Step 1: Configure a VLAN, and configure the link type of the ports.

#On Device, create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#On Device, configure the link type of port gigabitethernet0/1 to Access and allow services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the storm suppression function.

#On port gigabitethernet0/1 of Device, enable the storm suppression function, and the pps mode is used to suppress broadcast packets, and the suppression rate is 20pps.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#storm-control action shutdown
Device(config-if-gigabitethernet0/1)#storm-control broadcast pps 20
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Configure the Error-Disable function.

#Enable the storm suppression recovery function in Error-Disable, and set the recovery time to 30 seconds.

```
Device(config)#errdisable recovery cause storm-control
Device(config)#errdisable recovery interval 30
```

Step 4: Check the result.

#Query the configuration related to Error-Disable.

```
Device#show errdisable recovery

Error disable auto recovery config
interval:30 seconds
ErrDisable Reason   Timer Status
---------------     ------------
bpduguard           Disabled
dai                 Disabled
dhcp-snooping       Disabled
eips-udld           Disabled
l2pt                Disabled
link-flap           Disabled
loopback-detect     Disabled
oam                 Disabled
port-security       Disabled
storm-control       Enabled
ulfd                Disabled
```

#When PC sends a large number of broadcast packets, port gigabitethernet0/1 is closed, and the following information is printed:

```
Mar 29 16:16:24: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Mar 29 16:16:25: %PORTSTS: Storm occur on gigabitethernet0/1, ActionType:port storm shutdown.
stormType broadcast storm
```

#Query the status of port gigabitethernet0/1.

```
Device#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
    Description       :
    Status            : Enabled
    Link              : Down (Err-disabled)
    Set Speed         : Auto
    Act Speed         : Unknown
    Set Duplex        : Auto
    Act Duplex        : Unknown
    Set Flow Control : Off
    Act Flow Control : Off
    Mdix              : Auto
    Mtu               : 1824
    Port mode         : LAN
    Port ability      : 10M HD,10M FD,100M HD,100M FD,1000M FD
    Link Delay        : No Delay
    Storm Control     : Unicast Disabled
    Storm Control     : Broadcast Pps 20
    Storm Control     : Multicast Disabled
    Storm Action      : Shutdown
    Port Type         : Nni
    Pvid              : 2
    Set Medium        : Copper
    Act Medium        : Copper
    Mac Address       : 94ae.e354.5ca5
```

#After 30 seconds, port gigabitethernet0/1 will be enabled.

#Query the status of port gigabitethernet0/1.

```
Device#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
        Description      :
        Status           : Enabled
        Link             : Up
        Set Speed        : Auto
        Act Speed        : 1000
        Set Duplex       : Auto
        Act Duplex       : Full
        Set Flow Control : Off
        Act Flow Control : Off
        Mdix             : Auto
        Mtu              : 1824
        Port mode        : LAN
        Port ability     : 10M HD,10M FD,100M HD,100M FD,1000M FD
        Link Delay       : No Delay
        Storm Control    : Unicast Disabled
        Storm Control    : Broadcast Pps 20
        Storm Control    : Multicast Disabled
        Storm Action     : Shutdown
        Port Type        : Nni
        Pvid             : 2
        Set Medium       : Copper
        Act Medium       : Copper
        Mac Address      : 94ae.e354.5ca5
```

30 ARP

30.1 Overview

ARP provides dynamic mapping from IP addresses to MAC addresses. The Ethernet frames to be transmitted in the Ethernet can be encapsulated properly only after MAC addresses are specified. The ARP protocol is used to obtain MAC addresses that correspond to IP addresses.

30.2 ARP Function Configuration

Table 30-1 ARP Function List

Configuration Tasks	
Configure basic functions of ARP.	Configure a static ARP entry.
	Configure the maximum number of dynamic ARP entries.
	Configure the dynamic ARP aging time.
	Enable ARP dynamic learning.
	Configure the ARP receive queue depth.
	Configure ARP proxy.

30.2.1 Configure Basic Functions of ARP *-B -S -E -A*

Configuration Conditions

None

Configure a Static ARP Entry

Configuring static ARP means that a user manually specifies the mapping between IP addresses and MAC addresses.

Table 30-2 Configuring Static ARP

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure a static ARP entry.	**arp** [**vrf** *vrf-name*] { *ip-address* | *host-name* } *mac-address* [**alias** [**advertise**] | **advertise** [**alias**]]	Mandatory.

NOTE

- When the configured static ARP entry contains an alias, if an ARP request for this IP address is received, the MAC address in the static ARP entry is used for response.
- When the configured static ARP entry contains an advertise option, the static ARP will be regularly advertised when the static ARP advertisement is enabled.

Configure the Maximum Number of Dynamic ARP Entries

The purpose of configuring the maximum number of dynamic ARP entries is to prevent dynamically learned ARP from occupying too many system resources.

Table 30-3 Configuring the Maximum Number of Dynamic ARP Entries

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the maximum number of dynamic ARP entries.	**arp limited** *max-entries*	Mandatory. By default, the maximum number of dynamic ARP entries is 2000.

Configure the Dynamic ARP Aging Time

The life cycle of a dynamically learned ARP entry is the aging time. Within the aging time, the device sends ARP requests periodically. If it receives an ARP response, it resets the aging time. If the aging time expires, the device deletes the dynamic ARP entry.

Table 30-4 Configuring the Dynamic ARP Aging Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure the dynamic ARP aging time.	**arp timeout** { *second* | **disable** }	Mandatory. The default aging time is 1200 seconds.

Enable Dynamic ARP Learning

By default, a dynamic ARP learning is enabled on a device. To prevent dynamic learning from occupying too many system resources, you can disable the dynamic ARP learning function. After dynamic ARP learning is disabled, after the local device receives an ARP request for the MAC address of the local device, it sends an ARP response but does not generate any related ARP entry. An ARP entry is generated only when the local device requests for the MAC address of a peer device.

Table 30-5 Enabling Dynamic ARP Learning

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable dynamic ARP learning.	**arp learn-active**	Mandatory. By default, dynamic ARP learning is enabled.

Configure ARP Receive Queue Depth

The ARP packets received by the device will be first cached to the ARP receive queue. The system will read the packets from the queue in order and then handle the packets. When the cached ARP packets reach the queue depth, the subsequently received APR packets will be dropped. The user can adjust the ARP receive queue depth based on the network ARP emergency.

Table 30-6 Configure the ARP Receive Queue Depth

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the ARP receive queue depth	**arp queue-length** *length*	Mandatory The queue depth is 200 by default

Configure ARP Proxy

An ARP request is sent by the host of one network to another network, and the intermediate device between the two networks can respond to the ARP request. This process is called ARP proxy.

Table 30-7 Configuring ARP Proxy

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure ARP proxy.	**ip proxy-arp**	Mandatory. By default, the ARP proxy function is enabled.

30.2.2 ARP Monitoring and Maintaining *-B -S -E -A*

Table 30-8 ARP Monitoring and Maintaining

Command	Description
show arp [**vrf** *vrf-name*]	Queries the ARP table.
show arp attack-detection	Displays the information about the host which has been suspected of initiating ARP attacks.

30.3 ARP Typical Configuration Example

30.3.1 Configure ARP Proxy *-B -S -E -A*

Network Requirements

- Device is directly connected to PC1 and PC2 respectively. The network number of the LAN in which PC1 and PC2 is located is 10.0.0.0/16.
- The MAC address of the interface VLAN2 of Device is 94ae.e313.0102.
- Through the ARP proxy of Device, PC1 can successfully ping PC2, and PC1 can learn the MAC address of PC2.

Network Topology

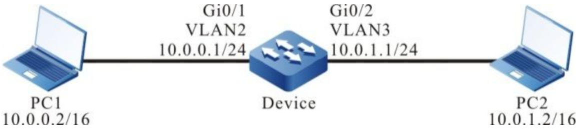


Figure 30-1 Networking for Configuring ARP Proxy

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs.(Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Check the result.

#Ping the PC2 IP address 10.0.1.2 from PC1.

```
C:\Documents and Settings>ping 10.0.1.2

Pinging 10.0.1.2 with 32 bytes of data:

Reply from 10.0.1.2: bytes=32 time<1ms TTL=255
Reply from 10.0.1.2: bytes=32 time<1ms TTL=255
Reply from 10.0.1.2: bytes=32 time<1ms TTL=255
Reply from 10.0.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.1.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#Query the ARP entry of Device.

```
Device#show arp
Protocol  Address     Age (min) Hardware Addr   Type    Interface   Swithport
Internet  10.0.0.1     -       94ae.e313.0102  ARPA    vlan2       ---
Internet  10.0.0.2     1       B8AC.6F2D.4498  ARPA    vlan2       gigabitethernet0/1
Internet  10.0.1.1     -       94ae.e313.0103  ARPA    vlan3       ---
Internet  10.0.1.2     1       4437.e603.0d63  ARPA    vlan3       gigabitethernet0/2
```

#Query the ARP entry of PC1.

```
C:\Documents and Settings>arp -a

Interface: 10.0.0.2 --- 0x5
  Internet Address      Physical Address      Type
  10.0.0.1              00-01-7a-13-01-02     dynamic
  10.0.1.2              00-01-7a-13-01-02     dynamic
```

#Ping from PC1 to PC2 is successful. The PC1 has learned the MAC address of PC2.

NOTE

- By default, ARP proxy is enabled for a device.

30.3.2 Configure a Static ARP Entry *-B -S -E -A*

Network Requirements

- Device and PC are directly connected.
- The MAC address of PC is 4437.e603.0d63.
- The IP address and MAC address of PC is bound to Device.
- PC can successfully ping the address of the interface VLAN2 of Device.

Network Topology

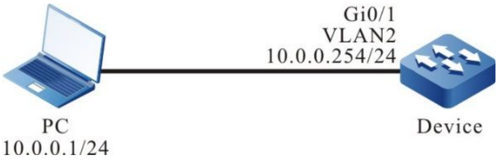


Figure 30-2 Networking for Configuring a Static ARP Entry

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs.(Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Bind the IP address and MAC address of PC to Device.

#Configure Device.

Bind the IP address and MAC address of PC to Device.

```
Device(config)#arp 10.0.0.1 4437.e603.0d63
```

Step 4: Check the result.

#Query the ARP entry of Device.

```
Device1#show arp
Protocol  Address     Age (min) Hardware Addr   Type    Interface  Switchport
Internet  10.0.0.1     -      4437.e603.0d63   ARPA    vlan2      gigabitethernet0/1
Internet  10.0.0.254  -      94ae.e313.0102   ARPA    vlan2      ---
```

#PC can successfully ping the address 10.0.0.254 of the interface VLAN2 of Device.

```
C:\Documents and Settings>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
                    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#PC can successfully ping the address of the interface VLAN2 of Device.

31 IP Basics

31.1 Overview

The Internet Protocol (IP) is based on datagrams. It is used in data exchange between computer networks. The protocols that are supported by the device include: IP, ICMP, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Socket.

Among them, IP packets are the base of the TCP/IP protocol stack. The IP layer is responsible for addressing, fragmentation, reassembly, and protocol information partitioning. As the network layer protocol, the IP protocol performs route addressing and control packet transmission.

The UDP protocol and the UDP protocol is set up based on the IP protocol. They provide connection-based reliable data transmission services and non-connection-based unreliable data transmission services respectively.

ICMP is mainly used to provide network detection services. It also provides an error report if the network layer or transmission layer protocol becomes abnormal, and it informs the related device of the abnormality to facilitate network control management.

31.2 IP Basic Function Configuration

Table 31-1 IP Basic Function List

Configuration Tasks	
Configure an IP address.	Configure an IP address for an interface.
	Configure an unnumbered IP address for an interface.
Configure basic functions of the IP protocol.	Configure the depth of the IP packet receiving queue.
	Configure the Time To Live (TTL) of transmitted IP packets.
	Configure timeout for packet reassembly.
	Enable IP packet receiving verification and check.
	Configure transmitted IP packets to calculate a checksum.

Configuration Tasks	
	Enable IP routing cache.
Configure basic functions of the ICMP protocol.	Enable global ICMP redirection.
	Enable global ICMP redirection.
	Enable ICMP destination unreachable.
	Configure ICMP rate limit.
Configure basic functions of the TCP protocol.	Configure the size of the TCP receiving cache.
	Configure the size of the TCP transmitting cache.
	Configure the maximum number of TCP retransmissions.
	Configure the maximum length of TCP packets.
	Configure the maximum TCP round-trip time.
	Configure the TCP connection idle time.
	Configure TCP connection setup waiting time.
	Configure the maximum number of TCP keep-alive times.
	Enable the TCP timestamp.
	Enable TCP selective retransmission.
Configure basic functions of the UDP protocol.	Configure TTL of UDP packets.
	Configure the size of the UDP receiving cache.
	Configure the size of the UDP transmitting cache.
	Enable UDP verification and check.
	Fill in UDP packet checksum.

31.2.1 Configure an IP Address *-B -S -E -A*

An IP address is a 32-bit number which uniquely identifies a network device that runs the IP protocol on the Internet.

An IP address consists of the following two parts:

- Network number (Net-id): It identifies the network in which the device is located.
- Host number (Host-id): It specifies the host number in the device network.

To facilitate IP address management, IP addresses are categorized into five classes, and each IP address class has its own functions. IP addresses of classes A to C are used for address allocation, IP addresses of class D is used in multicast applications, and IP addresses of class E are used for test purpose. The following table shows the IP addresses classes and their ranges.

Table 31-2 IP Address Classes and Their Ranges

Address Type	Available Network Address Range	Description
A	1.0.0.0-127.0.0.0	Network number 127 is used for loopback interfaces.
B	128.0.0.0-191.255.0.0	-
C	192.0.0.0-223.255.255.0	-
D	224.0.0.0-239.255.255.255	Class D addresses are used for multicast.
E	240.0.0.0-247.255.255.255	Class E addresses are used for test purpose.

With the development of the Internet, IP address resources have gradually been consumed up. Address allocation based on classes causes address waste, so the concept of "subnet" is introduced. "Subnet" takes some host numbers in the IP addresses as subnet numbers. In this way, a large network is divided into multiple subnets. This facilitates network planning and deployment.

The three address segments, 10.0.0.0-10.255.255.255, 172.16.0.0-172.16.255.255, and 192.168.0.0-192.168.255.255 are private and reserved addresses, and they cannot be allocated to the public network.

This section describes how to configure an interface IP address and how to configure an unnumbered interface IP address.

Configuration Conditions

None

Configure an IP Address for an Interface

An IP address can only be configured for an interface that supports the IP protocol. One interface can only be configured with one primary IP address but it can be configured with multiple secondary IP addresses.

Table 31-3 Configuring an IP Address for an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure an IP address for an interface.	**ip address** *ip-address* { *network-mask* | *mask-len* } [**secondary**]	Mandatory.

NOTE

- One interface can only be configured with one primary IP address, therefore, the newly configured primary IP address replaces the original primary IP address.
- Before an interface is configured with secondary IP addresses, the interface must be configured a primary IP address. An interface can be configured with a maximum of 100 secondary IP addresses.
- The IP addresses of different interfaces must not in the same network segment, but the primary and secondary IP addresses of one interface can be in the same network segment.

Configure an Unnumbered IP Address for an Interface

Unnumbered IP addresses save IP addresses. In the case of unnumbered IP addresses, the IP addresses of other interfaces can be borrowed instead of allocated independently. If an unnumbered interface generates an IP packet, the source IP address of the packet is the primary IP address of a borrowed interface. In configuring an unnumbered IP address for an interface, the interface to be borrowed must be specified, so that the IP address of the interface can be borrowed.

Table 31-4 Configuring an Unnumbered IP Address for an Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-

Step	Command	Description
Configure an unnumbered IP address for an interface.	**ip unnumbered** *reference-interface*	Mandatory.

NOTE

- The borrowed interface must be configured with the primary IP address, and the interface must not be configured with an unnumbered IP address.
- The primary IP address of an interface can be borrowed by multiple interfaces, but only the primary IP address of the interface can be borrowed.

31.2.2 Configure Basic Functions of the IP Protocol *-B -S -E -A*

In the TCP/IP protocol stack, the IP protocol is the network layer core protocol that is responsible for network interconnection. The IP protocol is a connectionless protocol. Before transmitting data, you need not set up a connection. The IP protocol tries best to deliver packets, but is does not ensure that all packets can reach the destination orderly.

Configuration Conditions

None

Configure the Depth of the IP Packet Receiving Queue

The IP packets received by a device are first cached in the IP packet receiving queue of an interface. The system reads packets orderly in the queue for processing. If the cached IP packets reach the specified queue depth, the later IP packets are discarded. You can adjust the depth of the IP packet receiving queue according to burst of IP packets in the network.

Table 31-5 Configuring the Depth of the IP Packet Receiving Queue

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the depth of the IP packet receiving queue to a specified value.	**ip option queue-length** *queue-size*	Mandatory. By default, the depth of the IP packet receiving queue is 200.
Configure the depth of the IP packet receiving queue to the default value.	**default ip option queue-length**	Optional.

Configure the TTL of Transmitted IP Packets

The header of an IP packet contains the Time-To-Live (TTL) field, which is decreased by one once the IP packet passes a routing device. When the TTL is 0, the device discards the IP packet. By default, the TTL of IP packets transmitted by the device is 255, that is, the packet can only be transmitted for up to 255 times. If you want to limit the number of packet forwarding times, adjust the TTL value for the transmitted IP packets.

Table 31-6 Configuring the TTL of Transmitted IP packets

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the TTL of transmitted IP packets to a specified value.	**ip option default-ttl** *ttl - value*	Mandatory. By default, the TTL of transmitted IP packets is 255.
Configure the TTL of transmitted IP packets to a default value.	**default ip option default-ttl**	Optional.

Configure Timeout for Packet Reassembly

If an IP packet is fragmented during the transmission, after the fragments reach the destination, they need to be reassembled to form a complete IP packet. Before all fragments are received, the received fragments are cached temporarily. If reassembly times out before all fragments reach the destination, the received fragments are discarded.

Table 31-7 Configuring Timeout for Packet Reassembly

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configuring timeout for packet reassembly to a specified value.	**ip option fragment-ttl** *ttl-value*	Mandatory. By default, the timeout for packet reassembly is 60, and the unit is 0.5 second.
Configuring timeout for packet reassembly to the default value.	**default ip option fragment-ttl**	Optional.

NOTE

- The unit for timeout of packet reassembly is 0.5 second.

Enable IP Packet Receiving Verification and Check

You can enable this function to verify and check the received IP packets. If the checksum is incorrect, the packet will be discarded.

Table 31-8 Enabling IP Packet Receiving Verification and Check

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable IP packet receiving verification and check.	**ip option recv-checksum**	Mandatory. By default, the function is enabled.
Configure the method for verifying and checking the received IP packets to the default value.	**default ip option recv-checksum**	Optional.

Enable IP Routing Cache

After a packet is sent from socket to the IP layer, if the destination address is the same as the previous packet and the route is valid, the packet directly use the route in the cache without the need of searching for another route.

Table 31-9 Enabling IP Routing Cache

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable IP routing cache.	**ip upper-cache**	Mandatory. By default, the IP routing cache function is enabled.

31.2.3 Configure Basic Functions of the ICMP Protocol *-B -S -E -A*

In the TCP/IP protocol stack, ICMP is mainly used to provide network detection services. It also provides an error report if the network layer or transmission layer protocol becomes abnormal, and it informs the related device of the abnormality to facilitate network control management.

Configuration Conditions

None

Enable Global ICMP Redirection

After a device receives an IP packet to be forwarded, if it is found that the receiving interface of the packet and the transmitting interface of the packet are the same through route selection, the device forwards the packet and sends back an ICMP redirection packet to the source end, requesting the source end to reselect the correct next hop for transmission of later packets. By default, a device can send ICMP redirection packets. In some special cases, you can prohibit a device from sending ICMP redirection packets.

Table 31-10 Enabling Global ICMP Redirection

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable global ICMP redirection.	**ip redirect**	Mandatory. By default, the global ICMP redirection function is enabled.

Enable Global ICMP Redirection

In sending ICMP redirection packets, if you need to send ICMP redirection packets, you need to enable the ICMP redirection function on the interface.

Table 31-11 Enabling Global ICMP Redirection

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Enable ICMP redirection on an interface.	**ip redirects**	Mandatory.

Step	Command	Description
		By default, the ICMP redirection function is enabled on an interface.

NOTE

- You can send ICMP redirection packets only when the ICMP redirection function is enabled globally and on the interface.

Enable ICMP Destination Unreachable

After a device receives IP datagrams, if the destination is unreachable, the packet is discarded and the ICMP destination unreachable error packet is sent back to the source end.

- If route selection of a forwarded IP packet fails, the host unreachable ICMP error packet is sent back to the source end.
- For an IP packet that can be forwarded, if you need to fragment the IP packet but a Don't Fragment (DF) bit is set in the packet, an ICMP error packet indicating that "segmentation is required but a DF bit is set" is sent to the source end.
- For an IP packet whose destination address is the local device, if the device does not support the upper-layer protocol of the device, it sends a "protocol unreachable" ICMP error packet to the source end.
- For an IP packet whose destination address is the local device, if the transport layer port of the packet of the packet does not match the port that the device process monitors, the device sends back a "port unreachable" ICMP error packet to the source end.

If a device encounters a malicious attack by a large number of ICMP destination unreachable packets, the device performance is degraded, and network traffic is increased. To prevent such case, you can disable the function of sending ICMP destination unreachable packets.

Table 31-12 Enabling ICMP Destination Unreachable

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Enable ICMP destination unreachable.	**ip unreachables**	Optional. By default, the ICMP destination unreachable function is enabled.

Configure ICMP Rate Limit

If a device encounters a malicious attack by a large number of ICMP error packets, the device performance is degraded, and network traffic is increased. To prevent such case, you can configure ICMP packet rate limit. The types of ICMP error packets include: unreachable packets, redirection packets, TTL timeout packets, and parameter error packets. The default rate limit of the packets is 10pps, while the transmitting rate of the other types of packets is 0, that is, no rate limit. In addition, you can configure the transmitting rates for different types of packets independently. If no rate is configured for a type of packets, the default value is used.

Table 31-13 Configuring ICMP Rate Limit

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable ICMP rate limit.	**ip icmp ratelimit enable**	Mandatory. By default, the function is enabled.
Configure ICMP rate limit.	**ip icmp ratelimit** { **default** *pps* | **echo-reply** { *pps* | **unlimit** } | **mask-reply** { *pps* | **unlimit** } | **param-problem** { *pps* | **unlimit** } | **redirect** { *pps* | **unlimit** } | **time-exceed** { *pps* | **unlimit** } | **time-stamp-reply** { *pps* | **unlimit** } | **unreach** { *pps* | **unlimit** } }	Mandatory. By default, the ICMP rate limit function is enabled.

31.2.4 Configure Basic Functions of the TCP Protocol *-B -S -E -A*

In the TCP/IP protocol stack, TCP is a connection-oriented transport layer protocol. Before sending data through the TCP protocol, you must first set up a connection. The TCP protocol provides congestion control and ensures reliable data transmission.

Configuration Conditions

None

Configure the Size of the TCP Receiving Cache

In some special network environment, you can configure both the size of receiving cache and the size of transmitting cache of a TCP connection so that the network can reach the optimal performance. If the TCP connection receiving cache is not configured, the size of the receiving cache is the default value.

Table 31-14 Configuring the Size of the TCP Receiving Cache

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the size of the TCP receiving cache.	**ip tcp recvbuffers** *buff-size*	Mandatory. By default, the size of the receiving cache is 8192 bytes.

Configure the Size of the TCP Transmitting Cache

In some special network environment, you can configure both the size of receiving cache and the size of transmitting cache of a TCP connection so that the network can reach the optimal performance. If the TCP connection transmitting cache is not configured, the size of the transmitting cache is the default value.

Table 31-15 Configuring the Size of the TCP Transmitting Cache

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the size of the TCP transmitting cache.	**ip tcp sendbuffers** *buff-size*	Optional. By default, the size of the transmitting cache is 8192 bytes.

Configure the Maximum Number of TCP Retransmissions

After the server sends a SYN-ACK packet, if it does not receive a response packet from the client, the server retransmits the packet. If the number of retransmissions exceeds the maximum number of retransmissions defined by the system, the system disconnects the TCP connection.

Table 31-16 Configuring the Maximum Number of TCP Retransmissions

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Configure the maximum number of TCP retransmissions.	**ip tcp retransmits** *retransmits-count*	Mandatory. By default, the maximum number of TCP retransmissions is 3.

Configure the Maximum Length of TCP Packets

The maximum length of TCP packets is the maximum length of data blocks that are sent by the transmitting end of a TCP connection to the receiving end. When a connection is set up, the smaller maximum packet length of the two ends is used as the maximum packet length in sending TCP packets by the two ends. If a TCP packet exceeds the maximum packet length, the transmitting ends fragments the packet before sending it.

Table 31-17 Configuring the Maximum Length of TCP Packets

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the maximum length of TCP packets.	**ip tcp segment-size** *seg-size*	Optional. By default, the maximum length of TCP packets is 512 bytes.

Configure the Maximum TCP Round-Trip Time

The TCP round trip time refers to the time between the timepoint at which the transmitting end sends a TCP packet and the timepoint at which the transmitting end receives the response packet. The maximum TCP round-trip time that is configured during TCP connection setup is taken as the initial value of the TCP round-trip time. The later TCP round-trip time is calculated according to the actual round-trip time. By default, the maximum TCP round-trip time is 3 seconds.

Table 31-18 Configuring the Maximum TCP Round-Trip Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the maximum TCP round-trip time.	**ip tcp round-trip** *round-trip-time*	Mandatory. By default, the maximum TCP round-trip time is 3 seconds.

Configure the TCP Connection Idle Time

After a TCP connection is set up, if no data is exchanged, the TCP connection idle time times out. Then TCP performs a keep-alive test. After the maximum number of keep-alive times is reached, the TCP connection is disconnected. By default, the TCP connection idle time is 2 hours.

Table 31-19 Configuring the TCP Connection Idle Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the TCP connection idle time.	**ip tcp idle-timeout** *idle-time*	Mandatory. By default, the TCP connection idle time is 14400, and the unit is 0.5 second.

NOTE

- The unit of the TCP connection idle time is 0.5 second.

Configure TCP Connection Setup Waiting Time

The setup of a TCP connection requires three handshakes. After a TCP client sends a connection request packet, it waits for the response from the TCP server before completing connection setup. After the time for waiting for connection setup timeout before a response is received, connection setup is terminated. By default, the time for waiting for setting up a TCP connection is 75 seconds.

Table 31-20 Configuring TCP Connection Setup Waiting Time

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure TCP connection setup waiting time.	**ip tcp init-timeout** *init-time*	Mandatory. By default, the time for waiting for setting up a TCP connection is 150 seconds, and the unit is 0.5 second.

NOTE

- The unit of the TCP connection setup waiting time is 0.5 second.

Configure the Maximum Number of TCP Keep-Alive Times

If no data is exchanged on a TCP connection for TCP connection idle time, a TCP keep-alive packet is sent for keep-alive test. If the keep-alive test fails, a keep-alive test is performed again. If the maximum number of TCP keep-alive times exceeds the threshold, the TCP connection will be disconnected. By default, the maximum number of TCP keep-alive times is 3.

Table 31-21 Configuring the Maximum Number of TCP Keep-Alive Times

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the maximum number of TCP keep-alive times.	**ip tcp keep-count** *keep-count*	Mandatory. By default, the maximum number of TCP keep-alive times is 3.

Enable the TCP Timestamp

TCP automatically calculates the packet round-trip time according to the serial number of the request packet and that of the response packet. However, the calculation is not accurate. Use of TCP timestamps can revise the problem. The transmitting end adds a timestamp into a packet, and the receiving end sends back the timestamp in the response packet. The transmitting end calculates the packet round-trip time according to the returned timestamp. By default, the function is disabled.

Table 31-22 Enabling the TCP Timestamp

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the TCP timestamp.	**ip tcp timestamp**	Mandatory. By default, the function is disabled.

Enable TCP Selective Retransmission

After TCP sends a series of packets, if the transmission of one packet fails, the series of packets need to be retransmitted. After TCP selective transmission is enabled, then only the packet that fails to be transmitted needs to be retransmitted. This reduces the system and line cost. By default, the function is disabled.

Table 31-23 Enabling TCP Selective Retransmission

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Configure TCP selective retransmission.	**ip tcp selective-ack**	Mandatory. By default, the function is disabled.

31.2.5 Configure Attack Defense Function of the TCP Protocol *-B -S -E -A*

If TCP server receives numerous SYN messages but the opposite end does not respond to the server's SYN+ACK reply. That will consume a lot of memory of the server and occupy the server's SYN queue, making the TCP server unable to serve normal requests. This kind of attacks can be avoided by configuring TCP attack defense function.

Configuration Conditions

None

Enable TCP syncache Function

When this function is enabled, the system does not rush to assign TCB upon receiving SYN datagram; instead, it replies a SYN ACK message first and saves the half-open connection information in a special HASH table (Cache) and then assign TCB until it receives correct response ACK message.

Table 2-24 Enable TCP syncache Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure TCP syncache function	**ip tcp syncache**	Required By default, the function is not enabled

Enable TCP syncookies Function

This function uses no memory resources at all. Instead, it uses a special algorithm to generate a Sequence Number. The algorithm takes into account the opposite side's IP, port, oneself's IP, and port's fixed information, and oneself's information which the other side does not know and which is relatively invariable, such as MSS and time, and, upon receiving the other side's ACK message, recalculates the Sequence Number to see whether it is identical to the Sequence Number-1 in the other side's reply message, thereby deciding whether or not to assign TCB resources.

Table 2-25 Enable TCP syncookies Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure TCP syncookies function	**ip tcp syncookies**	Required By default, the function is not enabled

31.2.6 Configure Basic Functions of the UDP Protocol ***-B -S -E -A***

In the TCP/IP protocol stack, UDP is a connectionless-oriented transport layer protocol. Before sending data through the TCP protocol, you need not set up a connection. The UDP protocol provides unreliable data transmission without congestion control.

Configuration Conditions

None

Configure TTL of UDP Packets

Configuring TTL of UDP packets means to fill in the TTL value in the IP header of UDP packets. The header of an IP packet contains the Time-To-Live (TTL) field, which is decreased by one once the IP packet passes a routing device. When the TTL is 0, the device discards the IP packet. By default, the TTL value of the IP packet of a UDP packet is 64.

Table 31-26 Configuring TTL of UDP Packets

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Configure TTL of UDP packets.	**ip udp default-ttl** *time-to-live*	Mandatory. By default, the TTL value of the IP packet of a UDP packet is 64.

Configure the Size of the UDP Receiving Cache

In some special network environment, you can configure both the size of receiving cache and the size of transmitting cache of a UDP connection so that the network can reach the optimal performance. If the

UDP connection receiving cache is not configured, the size of the receiving cache is the default value, 41600 bytes.

Table 31-27 Configuring the Size of the UDP Receiving Cache

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the size of the UDP receiving cache.	**ip udp recvbuffers** *buffer-size*	Mandatory. By default, the size of the UDP receiving cache is 41600 bytes.

Configure the Size of the UDP Transmitting Cache

In some special network environment, you can configure both the size of receiving cache and the size of transmitting cache of a UDP connection so that the network can reach the optimal performance. If the UDP connection transmitting cache is not configured, the size of the transmitting cache is the default value, 9216 bytes.

Table 31-28 Configuring the Size of the UDP Transmitting Cache

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the size of the UDP transmitting cache.	**ip udp sendbuffers** *buffer-size*	Mandatory. By default, the size of the UDP transmitting cache is 9216 bytes.

Enable UDP Verification and Check

To prevent errors that occur during transmission of UDP packets, after UDP packets are received, UDP verification and check need to be performed. The system compares the UDP packet verification field calculated by the receiving end and the UDP packet header checksum field. If the two values are different, the system determines that a transmission error has occurred, and then discards the packet. By default, the function is enabled.

Table 31-29 Enabling UDP Verification and Check

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Enable UDP verification and check.	**ip udp recv-checksum**	Mandatory. By default, the function is enabled.

Fill in UDP Packet Checksum

To prevent UDP packets from encountering transmission errors, in transmitting UDP packets, the transmitting end fills in the UDP packet checksum to be calculated into the UDP packet header checksum field for the receiving end to perform checksum check. By default, the function is enabled.

Table 31-30 Filling in UDP Packet Checksum

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure to fill in packet checksum in transmitting UDP packets.	**ip udp send-checksum**	Mandatory. By default, the function is enabled.

31.2.7 IP Basics Monitoring and Maintaining *-B -S -E -A*

Table 31-31 IP Basics Monitoring and Maintaining

Command	Description
clear ip icmpstat	Clears ICMP protocol statistics.
clear ip statistics	Clears IP protocol statistics.
clear ip tcpstat	Clears TCP protocol statistics.
clear ip udpstat	Clears UDP protocol statistics.
show ip icmpstat	Displays ICMP protocol statistics.
show ip interface [*interface-name* **|** **brief**]	Displays the interface IP address.

Command	Description
show ip sockets	Displays the Socket details.
show ip statistics	Displays IP protocol statistics.
show ip tcpstat	Displays TCP protocol statistics.
show ip udpstat	Displays UDP protocol statistics.
show tcp tcb [**detail**]	Displays TCP protocol control block details.

32 DHCP

32.1 Overview

It is hard to manage a large network. For example, in a network in which IP addresses are manually allocated, IP address conflicts are common. The only way of solving the problem is to dynamically allocate IP addresses to the hosts. The Dynamic Host Configuration Protocol (DHCP) allocates IP address to requesting hosts from an IP address pool. DHCP also provides other information, such as gateway IP and DNS server address. DHCP reduces the workload of the administrator in recording and tracking manually allocated IP addresses.

DHCP is a protocol that is based on UDP broadcast. The process for a DHCP client to obtain an IP address and other configuration information contains four phases.

DISCOVER phase. When the DHCP client accesses the network for the first time, it sends a DHCP DISCOVER packet with the source address 0.0.0.0 and destination address 255.255.255.255 to the network.

OFFER phase. After the DHCP server receives the DHCP DISCOVER broadcast packet sent by the client, it selects an IP address from the corresponding IP address pool according to the policy, and sends the IP address and other parameters to the client in a DHCP OFFER packet.

REQUEST phase. If the DHCP client receives response messages from multiple DHCP servers on the network, it selects one DHCP OFFER (usually the one that arrives first). Then it sends a DHCP REQUEST packet to the network, telling all DHCP servers the IP address of which server it will accept.

ACK phase. After the DHCP server receives the DHCP REQUEST packet from the DHCP server, it sends a DHCP ACK message containing the provided IP address and other configuration to the DHCP client, telling the DHCP client that the DHCP client can use the provided IP address.

The IP address that the DHCP server allocates to the DHCP client has a lease. After the lease expires, the server will take back the allocated IP address. When the lease term of the IP address of the DHCP client has passed half time, the DHCP client sends a DHCP REQUEST packet to the DHCP server requesting to update its IP address lease. If the DHCP server allows the DHCP client to use its IP address, the DHCP server responds with a DHCP ACK packet, requesting the DHCP client to update the lease. If the DHCP server does not allow the DHCP client to continue to use the IP address, the DHCP server responds with a DHCP NAK packet.

During dynamic IP address acquisition, request packets are sent in broadcast mode; therefore, DHCP is applied only when the DHCP client and server are in the same subnet. If multiple subnets exist in a network and the hosts of the subnets need to obtain configuration information such as IP address through the DHCP server, the hosts of the subnets communicate with the DHCP server through a DHCP relay to obtain IP addresses and other configuration information.

32.2 DHCP Function Configuration

Table 32-1 DHCP Function List

Configuration Tasks	
Configure a DHCP address pool.	Create a DHCP address pool.
	Bind an IP address to a DHCP host.
	Configure an IP address range.
	Configure a domain suffix.
	Configure the address of the NETBIOS server.
	Configure a DNS server address.
	Configure the default route.
	Configure the lease of an IP address.
	Configure VRF properties.
	Bind an IP address and a MAC address.
	Configure user-defined options.
Configure other parameters of a DHCP server.	Configure the range of reserved IP addresses.
	Configure DHCP ping detection parameters.
	Configure the DHCP service switch.
	Configure the DHCP packet transaction ID check switch.
Configure the functions of a DHCP client.	Configure a DHCP client.
Configure the function of a DHCP relay.	Configure a DHCP relay.
	Configure the Option82 function.

32.2.1 Configure a DHCP Address Pool *-S -E -A*

Configuration Conditions

None

Create a DHCP Address Pool

A DHCP server needs to select and allocate IP addresses and other parameters from a DHCP address pool. Therefore, a DHCP address pool must be created for the DHCP server.

Table 32-2 Creating a DHCP Address Pool

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create a DHCP address pool and enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	Mandatory. By default, no DHCP address pool has been created by the system.

NOTE

- Address pools fall into three types: Host, Network, and Range. The three types of address pools can be configured respectively through the host, network, and range commands.
- To modify the type of an address pool, delete the address pool type with the **no** command, and then configure it to another type.

Bind an IP Address to a DHCP Host

An address pool of the Host type has only one IP address, so a hardware address or client ID that matches a DHCP host must be configured. The DHCP server allocates the IP address from the address pool of the Host type only to the DHCP host that meets the specific conditions.

Table 32-3 Binding an IP Address to a DHCP Host

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Bind an IP address to a DHCP host.	**host** *ip-address* [*network- mask*]	Mandatory. By default, no IP address of any host is bound to a DHCP address pool.

Specify the address of hardware that matches the client.	**hardware-address** *ha*	Optional. By default, no address of hardware that matches the client is specified.
Specify a client ID.	**client-identifier** *cid*	Optional. By default, no client ID is specified for the DHCP address pool.

NOTE

- The **host** command is used to configure only one DHCP host address. A newly configured host address may overwrite the existing host address.
- If an address range has been configured for the address by using the **network** or **range** command, you must use the **no** command to delete the address range before use the **host** command for configuration.
- The **hardware-address** and **client-identifier** commands are only used for the address pool of the Host type, and at least one command must be used. They cannot be used for address pools of the Network type or the Range type.
- In the case of the **hardware-address** and **client-identifier** commands, only the last configured parameters take effect. Newly configured parameters overwrite the existing configuration parameters.

Configure an IP Address Range

On a DHCP server, each DHCP address pool must be configured with an IP address range to allocate IP addresses to DHCP clients.

Table 32-4 Configuring an IP Address Range

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Configure an IP address range for an address pool of the Network type.	**network** *ip-address* [*network- mask*]	Optional. By default, an IP address range is not configured for an address pool.

Configure an IP address range for an address pool of the Range type.	**range** *low-ip-addres high-ip-address* [*network-mask*]	Optional. By default, an IP address range is not configured for an address pool.

NOTE

- After an IP address range is configured for an address pool by using the **network** or **range** command, if you run the **network** or **range** command again, the new IP address range configuration overwrites the existing configuration.

Configure a Domain Suffix

On a DHCP server, you can configure a domain suffix respectively for each DHCP address pool. When a DHCP server allocates an IP address for a DHCP client, it also sends the domain suffix to the client.

When the DHCP client uses the domain name, you can input only part of the domain name while the system automatically adds the domain suffix for domain name resolution.

Table 32-5 Configuring a Domain Suffix

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Configure a domain for a client.	**domain-name** *domain-name*	Mandatory. By default, no domain name is configured.

Configure the Address of the NETBIOS Server

A DHCP client that runs on the Windows Operating System (OS) can obtain a mapping from the host name to the IP address from the WINS server through the NETBIOS protocol.

On a DHCP server, you can configure the NETBIOS server address respectively for each DHCP address pool. The DHCP server specifies the NETBIOS server address when it allocates an IP address for a client.

Table 32-6 Configuring the Address of the NETBIOS Server

Step	Command	Description

Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Configure the address of the NETBIOS server.	**netbios-name-server** *ip-address*&<1-8>	Mandatory. By default, the NETBIOS server address is not configured.

Configure a DNS Server Address

On a DHCP server, you can configure the DNS server address respectively for each DHCP address pool. When a DHCP server allocates an IP address for a DHCP client, it also sends the DNS server address to the client.

When the DHCP client starts dynamic domain name resolution, it queries the DNS server.

Table 32-7 Configuring a DNS Server Address

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Configure a DNS server address.	**dns-server** { *ip-address*&<1-8> | *auto-config* }	Mandatory. By default, the DNS server address is not configured.

Configure the Default Route

On a DHCP server, you can specify the address of a gateway corresponding to clients for each DHCP address pool. When the server allocates an IP address to a client, it also sends the gateway address to the client.

When a DHCP client accesses a server or host that is not in the network segment, its data is forwarded through the gateway.

Table 32-8 Configuring the Default Route

Step	Command	Description

Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Configure the default route.	**default-router** *ip-address*&<1-8>	Mandatory. By default, no default route is configured.

Configure the Lease of an IP Address

The IP address that the DHCP server allocates to the DHCP client has a lease. After the lease expires, the server will take back the allocated IP address. If the DHCP client wants to continue to use the IP address, it must have the IP address lease updated.

On the DHCP server, you can configure an IP address lease for each DHCP address pool.

Table 32-9 Configuring the Lease of an IP Address

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Configure an IP address lease.	**lease** *days* [*hours* [*minutes*]]	Mandatory. By default, the value of *days* is 1, the value of *hours* is 6, and the value of *minutes* is 0.

Configure VRF Properties

Virtual Route Forwarding (VRF) is a basic concept of the Multi Protocol Label Switching (MPL) Layer 3 Virtual Private Network (L3 VPN) network technology. Each VRF can be regarded as a virtual router which has an independent routing table. In addition, VRF has independent address space, a group of interfaces that belong to the VRF, and a group of routing protocols that are applied only to the VRF. The VRF technology is used to isolate different VPN users and solve the problem of network address overlapping.

Table 32-10 Configuring VRF Properties

Step	Command	Description

Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Configure VRF properties.	**vrf** vrf-name	Mandatory. By default, an address pool is not configured with VRF properties.

Bind an IP Address and a MAC Address

After IP addresses and MAC addresses are bound, when the client with a specified MAC address sends an IP address request to the DHCP server, the DHCP server allocates the IP address that is bound to the IP address to the client. In this way, as long as the MAC address of the client is not changed (by replacing the network adapter), the client will obtain the same IP address from the server each time.

Table 32-11 Binding IP Addresses and MAC Addresses

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-
Bind an IP address and a MAC address.	**bind** { *ip-address mac-address* **| automatic | lease** }	Mandatory. By default, no IP address and MAC address binding is configured.

Configure User-Defined Options

For some options, RFC does not give specifications; therefore, you can define these options according to the actual requirement.

Table 32-12 Configuring User-Defined Options

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Enter the DHCP configuration mode.	**ip dhcp pool** *pool-name*	-

Configuring user-defined options.	**option option-code** { **ascii** *ascii-string* **|** **hex** *hex-string* **|** **ip** *ip-address*&<1-8> }	Mandatory. By default, user-defined options are not configured.

32.2.2 Configure Other Parameters of a DHCP Server *-S -E -A*

Configuration Conditions

None

Configure the Range of Reserved IP Addresses

In a DHCP address pool, some IP addresses are reserved for some special devices, and some IP addresses conflict with the IP addresses of other hosts in the network. Therefore, the IP addresses cannot be dynamically allocated.

Table 32-13 Configuring the Range of Reserved IP Addresses

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the range of reserved IP addresses.	**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]	Mandatory. By default, the range of reserved IP addresses is not configured. The IP addresses in the reserved IP address range will not be allocated.

Configure DHCP Ping Detection Parameters

To prevent an IP address conflict, before dynamically allocating an IP address to a DHCP client, a DHCP server must detect the IP address. The detection operation is performed through the ping operation. The DHCP server determines whether an IP address conflict exists by checking whether an ICMP echo response packet is received within the specified time.

Table 32-14 Configuring DHCP Ping Detection Parameters

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Configure DHCP ping detection parameters.	**ip dhcp ping** { **packets** *packet-num* **| timeout** *time* }	Mandatory. By default, the number of ping packets is 1, and the timeout time is 50 ms.

Configure the DHCP Service Switch

You can control whether to provide the DHCP service through the DHCP service switch.

Table 32-15 Configuring the DHCP Service Switch

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Configure DHCP ping detection parameters.	**ip dhcp service**	Mandatory. By default, the DHCP service is enabled.

Configure DHCP Packet Transaction ID Check Switch

For some DHCP clients, their transaction ID of the DHCP-REQUEST packet may be different from the transaction ID of the previous DHCP-DISCOVER packet. Therefore, the switch is used to control whether to check the transaction ID of the DHCP-REQUEST packet.

Table 32-16 Configure the DHCP Packet Transaction ID Check Switch

Step	**Command**	**Description**
Enter the global configuration mode	**configure terminal**	-
Configure the DHCP ping parameter sniffing	**ip dhcp check-xid disable**	Mandatory By default, turn on the DHCP-REQUEST packet transaction ID check switch.

32.2.3 Configure the Functions of a DHCP Client *-S -E -A*

Configuration Conditions

None

Configure a DHCP Client

A DHCP client interface obtains an IP address and other parameters through DHCP.

Table 32-17 Configuring a DHCP Client

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure the DHCP client to obtain an IP address.	**ip address dhcp** [**request-ip-address** *ip-address*]	Mandatory. By default, the DHCP client is not configured to obtain an IP address.

32.2.4 Configure the Function of a DHCP Relay *-S -E -A*

Configuration Conditions

None

Configure a DHCP Relay

If multiple subnets exist in a network and the hosts of the subnets need to obtain configuration information such as IP address through the DHCP server, the hosts of the subnets communicate with the DHCP server through a DHCP relay to obtain IP addresses and other configuration information. If an interface is configured to work in DHCP relay mode, after the interface receives DHCP packets from a DHCP client, it relays the packet to the specified DHCP server. The DHCP server then allocates an IP address.

Table 32-18 Configuring a DHCP Relay

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the DHCP relay function.	**ip dhcp-server** *ip-address* [**vrf** *vrf-name*]	Mandatory.

		By default, the DHCP relay function is not configured.
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure the DHCP relay function.	**ip dhcp-server** *ip-address*&<1-3>	Mandatory. By default, the DHCP relay function is not configured.

Configure the Option82 Function

Option82 is a trunk information option, which records the location of a DHCP client. If a DHCP relay receives a request packet sent by a DHCP client to a DHCP server, it adds Option82 into the request packet and sends the packet to the DHCP server. If the DHCP relay receives a DHCP response packet which contains Option82, it deletes Option82 and forwards the packet to the DHCP client.

Table 32-19 Configuring the Option82 Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the Option82 function.	**ip dhcp relay information** { **option | remote-id** *interface-name* }	Mandatory. By default, the Option82 function is not configured.

32.2.5 DHCP Monitoring and Maintaining *-S -E -A*

Table 32-20 DHCP Monitoring and Maintaining

Command	Description
clear ip dhcp binding	Clears address binding from the DHCP server.
clear ip dhcp pool	Clears IP and MAC address binding from a DHCP address pool.
clear ip dhcp relay statistics	Clears statistics from the relay server.

show ip dhcp binding	Displays the lease information on the DHCP server.
show ip dhcp excluded-pool	Displays the reserved IP address range in the system.
show ip dhcp lease	Displays the lease information of DHCP clients.
show ip dhcp ping	Displays the ping parameters that are used by the DHCP server to perform address validity check.
show ip dhcp pool [*pool-name*]	Displays the configuration information of a DHCP address pool in the system.
show ip dhcp pool-binding	Displays the number of IP and MAC bindings.
show ip dhcp pool-statistic	Displays the statistics of DHCP address pools in the system.
show ip dhcp relay statistics	Clears statistics on the relay server.

32.3 DHCP Typical Configuration Example

32.3.1 Configure a DHCP Server to Statically Allocate IP Addresses *-S -E -A*

Network Requirements

- Device acts as a DHCP server to allocate IP addresses, gateway IP addresses, and DNS server IP addresses in a static manner.
- The DHCP server allocates an IP address to PC1 in MAC binding mode, and it allocates an IP address to PC2 in Client ID binding mode.

Network Topology

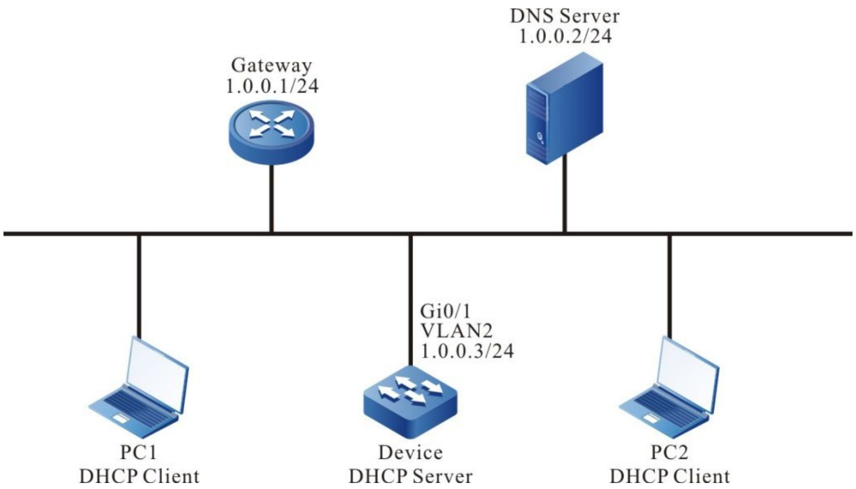


Figure 32-1 Configuring a DHCP Server to Statically Allocate IP Addresses

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure statically bound address pools and parameters.

#Configure the address pool mac-binding, and allocate an IP address to PC1 in static MAC binding mode.

```
Device#configure terminal
Device(config)#ip dhcp pool mac-binding
Device(dhcp-config)#host 1.0.0.11 255.255.255.0
Device(dhcp-config)#hardware-address 00e0.00c1.013d
Device(dhcp-config)#default-router 1.0.0.1
Device(dhcp-config)#dns-server 1.0.0.2
```

#Configure the address pool client-id-binding, and allocate an IP address to PC2 in static client ID binding mode.

```
Device#configure terminal
Device(config)#ip dhcp pool client-id-binding
Device(dhcp-config)#host 1.0.0.12 255.255.255.0
Device(dhcp-config)#client-identifier 0100.e04c.113c.f2
Device(dhcp-config)#default-router 1.0.0.1
Device(dhcp-config)#dns-server 1.0.0.2
```

Step 4: Check the result.

#On Device, use the **show ip dhcp binding** command to display the IP addresses that are allocated to PC1 and PC2.

```
Device#show ip dhcp binding
Current DHCP binding information

Hardware-Address          IP-Address      Lease              Status
00e0.00c1.013d          1.0.0.11        1Day 05:59:38       ACKED
00e0.4c11.3cf2          1.0.0.12        1Day 05:59:41       ACKED
```

On PC1 and PC2, check whether the obtained IP addresses, gateway IP addresses, and DNS server IP addresses are correct.

32.3.2 Configure a DHCP Server to Dynamically Allocate IP Addresses

-S -E -A

Network Requirements

- Two interface VLANs of Device, VLAN2 and VLAN3, are respectively configured with IP addresses in the 1.0.0.3/24 and 2.0.0.3/24 network segments.
- The DHCP server Device dynamically allocates IP addresses in the 1.0.0.0/24 and 2.0.0.0/24 network segments to the two clients in the directly-connected physical network.
- The IP addresses in network segment 1.0.0.0/24 have a one-day lease, the gateway address is 1.0.0.3, the DNS server address is 2.0.0.4, and there is no Winds server. The IP addresses in network segment 2.0.0.0/24 have a three-day lease the gateway address is 2.0.0.3, the DNS server address is 2.0.0.4, and the Wins server address is 2.0.0.5.
- The first 10 IP addresses in network segments 1.0.0.0/24 are reserved and cannot be allocated, and the domain suffix in the network segments is xxyyzz.com.

Network Topology

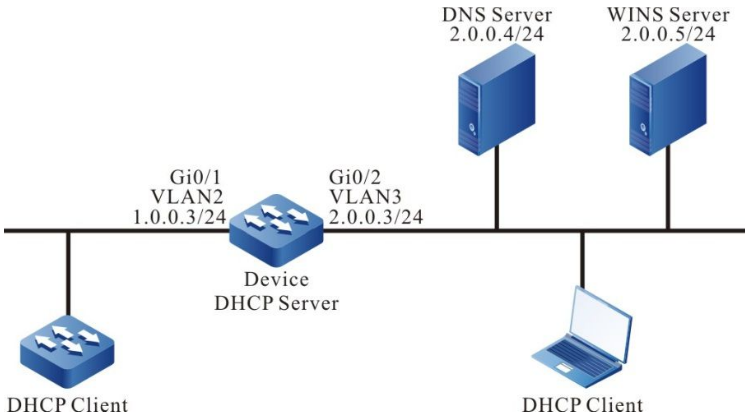


Figure 32-2 Networking for Configuring DHCP to Dynamically Allocate IP Addresses

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: On the DHCP server Device, configure two dynamic address pools and their parameters.

#Configure the first 10 IP addresses in the two address pools to be reserved.

```
Device#configure terminal
Device(config)#ip dhcp excluded-address 1.0.0.1 1.0.0.10
Device(config)#ip dhcp excluded-address 2.0.0.1 2.0.0.10
```

#Configure address pool dynamic-pool1 and its parameters (including address range, gateway, DNS, address lease, and local domain name).

```
Device#configure terminal
Device(config)#ip dhcp pool dynamic-pool1
Device(dhcp-config)#network 1.0.0.0 255.255.255.0
Device(dhcp-config)#default-router 1.0.0.3
Device(dhcp-config)#dns-server 2.0.0.4
Device(dhcp-config)#domain-name xxyyzz.com
Device(dhcp-config)#lease 1 0 0
Device(dhcp-config)#exit
```

#Configure address pool dynamic-pool2 and its parameters (including address range, gateway, DNS address, address lease, Wins server address, and local domain name).

```
Device#configure terminal
Device(config)#ip dhcp pool dynamic-pool2
Device(dhcp-config)#network 2.0.0.0 255.255.255.0
Device(dhcp-config)#default-router 2.0.0.3
Device(dhcp-config)#dns-server 2.0.0.4
Device(dhcp-config)#netbios-name-server 2.0.0.5
Device(dhcp-config)#domain-name xxyyzz.com
Device(dhcp-config)#lease 3 0 0
Device(dhcp-config)#exit
```

Step 4:   Check the result.

#On Device, query the IP addresses that are allocated to clients.

```
Device#show ip dhcp binding
Current DHCP binding information

Hardware-Address          IP-Address      Lease              Status
 0010.9400.94ae          2.0.0.11        2Day 23:59:52        ACKED
 00e0.00c1.013d          1.0.0.13        23:59:28           ACKED
```

#On Device, query the IP address pool allocation statistics.

```
Device#show ip dhcp pool-statistic
DHCP pool statistic

pool name                    free address    allocated address    total
---------                ------------   -----------------   -----
dynamic-pool1                  243           1                 244
dynamic-pool2                  243           1                 244

Free address: 486    Allocated address: 2    Total: 488
Total 20 address excluded
```

On the DHCP clients, query whether the IP addresses have been obtained properly.

NOTE

- The IP addresses in the address pool must be within the network segment range of the interface that provides the service.

32.3.3 Configure a DHCP Relay *-S -E -A*

Network Requirements

- The DHCP clients and the DHCP server are not in the same physical network.
- The DHCP clients are in network segment 1.0.0.0/24, and the DHCP server is in network segment 2.0.0.0/24.
- The IP address of the DHCP server Device1 is 2.0.0.1.
- The address pool of the DHCP server provides services to the client in network segment 1.0.0.0/24, and the first 10 IP addresses are reserved.
- The DHCP server allocates IP addresses to the DHCP clients that are in different physical networks by use of a DHCP relay.
- Device2 acts as the DHCP relay.

Network Topology

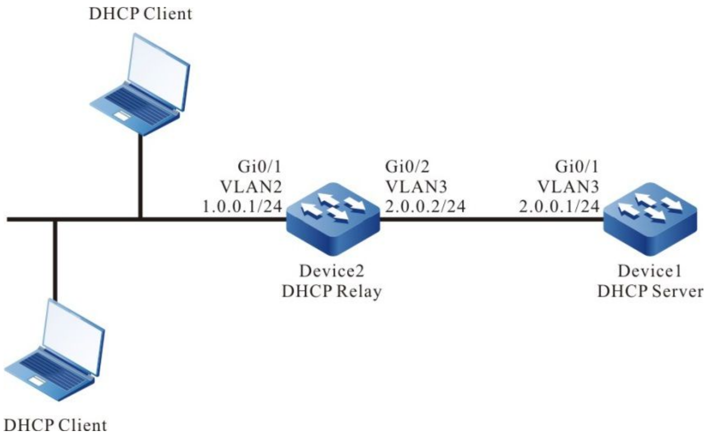


Figure 32-3 Networking for Configuring a DHCP Relay

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure an IP address pool for the DHCP server Device 1, and configure the reserved IP addresses.

#Configure IP addresses which are from 1.0.0.1 to 1.0.0.10 not to be allocated.

```
Device1#configure terminal
Device1(config)#ip dhcp excluded-address 1.0.0.1 1.0.0.10
Device1(config)#exit
```

#Configure IP address pool dynamic-pool for Device1.

```
Device1#configure terminal
Device1(config)#ip dhcp pool dynamic-pool
Device1(dhcp-config)#network 1.0.0.0 255.255.255.0
Device1(dhcp-config)#default-router 1.0.0.1
Device1(dhcp-config)#lease 1 0 0
Device1(dhcp-config)#exit
```

#Configure a static route to network segment 1.0.0.0/24.

```
Device1#configure terminal
Device1(config)#ip route 1.0.0.0 255.255.255.0 2.0.0.2
Device1(config)#exit
```

Step 4: On the DHCP relay, configure the IP address of the DHCP relay server to 2.0.0.1.

```
Device2#configure terminal
Device2(config)#ip dhcp-server 2.0.0.1
Device2(config)#exit
```

Step 5: Check the result.

#On Device1, query the IP addresses that have been allocated.

```
Device1#show ip dhcp binding
Current DHCP binding information

Hardware-Address          IP-Address      Lease              Status
 0010.9400.94ae          1.0.0.12       23:57:44           ACKED
```

Use the show ip dhcp binding command to query the IP addresses that have been allocated to clients. The result shows that a client has obtained the IP address 1.0.0.12.

32.3.4 Configure the DHCP Relay to Support Option82 *-S -E -A*

Network Requirements

- On the DHCP relay device, Option82 is enabled.
- For request packets that contain Option82, the processing policy keeps unchanged.
- For Option82 sub-option Remote ID, interface VLAN2 is specified.
- The DHCP relay Device adds Option82 in a request packet and forwards the request to DHCP server. The DHCP server then allocates IP addresses in the 1.0.0.0/24 network segment to the client.

Network Topology

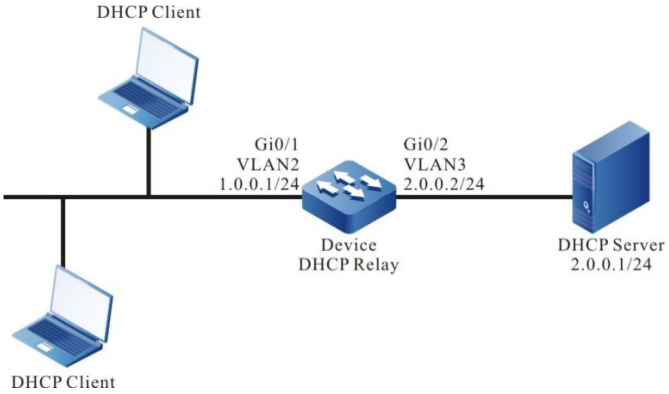


Figure 32-4 Networking for Configuring the DHCP Relay to Support Option82

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure the DHCP server.(Omitted)

Step 4: Configure the DHCP relay Device and Option82 parameters.

#Set the IP address of the relay server to 2.0.0.1.

```
Device#configure terminal
Device(config)#ip dhcp-server 2.0.0.1
Device(config)#exit
```

#Enable Option82, and set sub-option Remote-ID to VLAN2.

```
Device#configure terminal
Device(config)#ip dhcp relay information option
Device(config)#ip dhcp relay information remote-id vlan 2
Device(config)#exit
```

Step 5: Check the result.

On the DHCP client, query the IP address that the network adapter has obtained from network segment 1.0.0.0/24.

NOTE

- After Option82 is enabled, it sub-option Circuit ID is filled with the receiving interface index and the system ID of the relay device.

33 DNS

33.1 Overview

Domain Name System (DNS) is a distributed database that maps domain names and IP addresses. It provides conversion between domain names and IP addresses. With the use of DNS, when users access the Internet, they can use easy-to-memory and meaningful domain names. Then the domain name server in the network resolves the domain names into correct IP addresses. DNS is categorized into static DNS and dynamic DNS.

Static domain name resolution is conducted through a static DNS table. In the static DNS table, domain names and IP addresses are mapped, and some frequently used domain names are added. When a client requests for the IP address of a domain name, the DNS server first searches static DNS table for the corresponding IP address. This improves the efficiency of domain name resolution.

Dynamic domain name resolution is implemented by querying the DNS. A DNS client sends a domain name resolution request to a DNS server. After the DNS server receives the domain name resolution request, it first determines whether the requested domain name is located in its authorized management sub-domain. If yes, it searches the database for the required IP address and then sends the query result to the client. If the domain name is not in the authorized management sub-domain, the DNS server starts a recursive resolution with other DNS server, and then it sends the resolution result to the client. Alternatively, it specifies the address of the next DNS server in the response packet to the DNS client. Then, the client sends another domain name resolution request to the domain name server. This is so called iterative resolution mode.

33.2 DNS Function Configuration

Table 33-1 DNS Function List

Configuration Tasks	
Configure the DNS client function.	Configure static domain name resolution.
	Configure dynamic domain name resolution.

33.2.1 Configure the DNS Cache Specifications *-B -S -E -A*

Configuration Conditions

None

Configure DNS Specifications

When changing the maximum specifications supported by DNS, if the current specification is M and current quantity is n, and the configured specification is N, there could be the following scenarios:

1. Static specifications: if N > M or n < N < M; then the configuration will take effect immediately; if N < n, then the system will prompt a configuration failure message
2. Dynamic specifications: if N > M or n < N < M, then the configuration will take effect immediately; if N < n, the configuration will take effect and wait for the aging of dynamic quantity.

Table 33-2 Configure Privilege Mode Authentication Method List

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the maximum number of supportable specifications of static dns	**dns static max-count** *number*	Optional By default, the static cache supports up to 64
Configure the maximum number of supportable specifications of dynamic dns cache	**dns dynamic max-count** *number*	Optional By default, dynamic cache supports up to 10K

33.2.2 Configure the DNS Client Function *-B -S -E -A*

Configuration Conditions

None

Configure Static Domain Name Resolution

In configuring static domain name resolution, you can configure a domain names to map an IPv4 address.

Table 33-3 Configuring Static Domain Name Resolution

Step	**Command**	**Description**
Enter the global configuration mode.	**configure terminal**	-
Configure a domain name to map an IP address.	**ip host** [**vrf** *vrf-name*] *domain-name ip-address*	Mandatory. By default, no domain name and its

Step	Command	Description
		corresponding IP address is configured.

Configure Dynamic Domain Name Resolution

In configuring dynamic domain name resolution, you need to configure the IP address of a domain name server. Then, domain resolution requests can be sent to the proper domain server for resolution.

Users can pre-configure a domain suffix. Then, when the users use a domain name, they can input only part fields of the domain name, and the system automatically adds pre-configured domain suffix for resolution.

Table 33-4 Configuring Dynamic Domain Name Resolution

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure a domain suffix.	**ip domain-name** [**vrf** *vrf-name*] *domain-name*	Mandatory. By default, no domain suffix is configured.
Configure a DNS server address.	**ip name-server** [**vrf** *vrf-name*] *ip-address*	Mandatory. By default, the DNS server address is not configured.
Configure domain name resolution order.	**ip name-order** { **dns-first** | **dns-only** | **local-first** }	Optional. By default, the system resolution order is local-first.

33.2.3 Configure the DNS Detection Function *-B -S -E -A*

Configuration Conditions

None

Configure Domain Name List

By configuring the domain name list, the user can add and save some frequently used domain names in the domain name list. When it is time to use the domain names, simply specify the name in the domain name list will do.

Table 33-5 Configure Domain Name List

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create domain name list and enter domain name list configuration mode	**dns domain-list** *list-name*	Required By default, no domain name list is configured
Configure domain name	**domain** *domain-name*	Required By default, no domain name has been configured in the domain name list

Detect Resolution of Domain Name

By detecting the resolution of domain names, it is possible to decide whether the DNS server can resolute the specified domain name or not.

Table 33-6 Detect Resolution of Domain Name

Steps	Command	Description
Detect resolution of domain name	**dns query** [**vrf** *vrf-name*] *ip-address* [**name** *domain-name* **|** **name-list** *list-name*] [**timeout** *time*]	Required By default, domain name resolution is not tested

33.2.4 DNS Monitoring and Maintaining *-B -S -E -A*

Table 33-7 DNS Monitoring and Maintaining

Command	**Description**
clear hosts dynamic	Clear the dynamic domain name entry.

Command	Description
show hosts	Displays the information about the DNS table.
show name-server	Displays the DNS configuration information.

33.3 DNS Typical Configuration Example

33.3.1 Configure Static Domain Name Resolution *-B -S -E -A*

Network Requirements

- Device and PC are interconnected, and the route is reachable.
- The host name of PC is host.xxyyzz.com, and the IP address is 1.0.0.2/24.
- On Device, access the host host.xxyyzz.com through static domain name resolution.

Network Topology

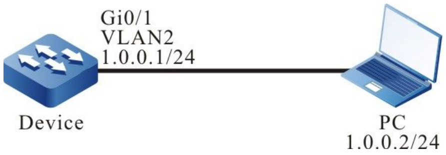


Figure 33-1 Networking for Configure Static Domain Name Resolution

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure a static domain name.

#On Device, configure the host name host.xxyyzz.com to correspond to IP address 1.0.0.2.

```
Device#configure terminal
Device(config)#ip host host.xxyyzz.com  1.0.0.2
Device(config)#exit
```

Step 4: Check the result.

#On Device, ping host host.xxyyzz.com. Device obtains the IP address 1.0.0.2 that corresponds to the host name through local domain name resolution.

```
Device#ping host.xxyyzz.com
```

```
Translating "host.xxyyzz.com" for IPv6
% Unrecognized host or address, or protocol not running.

%Bad IPv6 address or unknown hostname!


Translating "host.xxyyzz.com" for IPv4

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/6/16 ms.
```

NOTE

- In pinging a host name, the IPv6 address corresponding to the host name is first resolved, and then the IPv4 address.

33.3.2 Configure Dynamic Domain Name Resolution *-B -S -E -A*

Network Requirements

- The IP address of the DNS server is 1.0.0.3/24, the IP address of Device is 1.0.0.1/24, and the IP address of PC is 1.0.0.2/24.
- The DNS server, Device, and PC are interconnected through a LAN, and the route is reachable. On the DNS server, the DNS record of host.xxyyzz.com and 1.0.0.2 exists.
- Device access PC through dynamic resolution of host.xxyyzz.com through the DNS server.

Network Topology

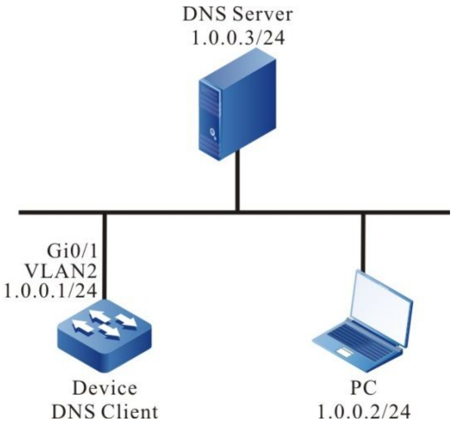


Figure 33-2 Networking for Configure Dynamic Domain Name Resolution

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure the DNS server.(Omitted)

Step 4: Configure the DNS client.

#Specify a DNS server for the client, and the IP address is 1.0.0.3.

```
Device#configure terminal
Device(config)#ip name-server 1.0.0.3
```

Step 5: Check the result.

#On Device, ping host host.xxyyzz.com. Device obtains the IP address 1.0.0.2 that corresponds to the host name through the DNS server.

```
Device#ping host.xxyyzz.com
Translating "host.xxyyzz.com" for IPv6
    Querying server (# 1) address = 1.0.0.3
    Querying server (# 1) address = 1.0.0.3
    Querying server (# 1) address = 1.0.0.3
% Unrecognized host or address, or protocol not running.

%Bad IPv6 address or unknown hostname!


Translating "host.xxyyzz.com" for IPv4
    Querying server (# 1) address = 1.0.0.3 [OK]


Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
```

Success rate is 100% (5/5). Round-trip min/avg/max = 0/6/16 ms.

34 IPv6 Fundamentals

34.1 IPv6 Fundamentals Overview

IPv6 (Internet Protocol Version 6, the second generation of network layer protocol, is also referred to as IPng (IP Next Generation). It is an upgraded version of IPv4 designed by IETF (Internet Engineering Task Force).

34.2 IPv6 Basic Function Configuration

Table 34-1 Fundamental Function Configuration List IPv6

Configuration task	
Configure IPv6 address	Configure interface IPv6 address
Configure basic functions of IPv6	Turn on IPv6 unicast forwarding function
	Turn on interface IPv6 function
	Configure IPv6 message hop limit value
	Configure interface's IPv6 MTU
Configure IPv6 neighbor discovery protocol	Configure IPv6 static neighbor
	Configure the aging time of STALE status IPv6 neighboring table entry
	Configure NS message's time interval for retransmission
	Configure the number of NS messages sent during IPv6 duplicate address detection
	Configure RA message related parameters
	Turn on interface send redirect message function
	Configure ICMPv6 error message send rate

Configuration task	
Configure ICMPv6 function	Turn on ICMPv6 destination unreachable message sending function
Configure IPv6 TCP attack defense function	Turn on TCP syncache function
	Turn on TCP syncookies function

34.2.1 figure Interface IPv6 Address *-B -S -E -A*

The most significant difference between IPv4 and IPv6: the length of IP address is 32bit for the former and increased to 128bit for the latter. IPv6 addresses are expressed as a series of 16bit hexadecimal numbers separated by colon(:). Each IPv6 address is divided into 8 groups of 16 bits separated by a colon, each of the 16-bit group is expressed as a 4-digit hexadecimal number, for example: 2000:0000:240F:0000:0000:0CB0:123A:15AB.

In order to simplify the expression of IPv6 addresses, the 0 in an IPv6 address can be handled in any of the following ways:

- Precursor 0(s) in every group can be omitted, for example, the above-mentioned address can be expressed as: 2000:0:240F:0:0:CB0:123A:15AB.
- If an address contains 2 or more consecutive all-0 groups, such groups can be replaced by a double-colon(::), for example, the above-mentioned address can be expressed as 2000:0:240F::CB0:123A:15AB.
- In an IPv6 address, double-colon(::) can be used only once; otherwise, the Device will not be able to determine the number of 0s represented by the :: when converting :: back to 0s in order to restore the 128-bit address.

An IPv6 address consists of two parts: address prefix and interface identifier. The address prefix is equivalent to the net-id field of an IPv4 address, interface identifier is equivalent to the host-id field of an IPv4 address.

IPv6 address prefix is expressed as: IPv6 address/prefix length. IPv6 address can be in any of the afore-mentioned forms, prefix length is a decimal number which denotes how many bits of the IPv6 address are the address prefix.

IPv6 addresses can be divided into three types: unicast addresses, multicast addresses and anycast addresses.

- Unicast addresses: used to identify one and only one interface, similar to the unicast addresses in IPv4. Datagrams sent to a unicast address will be sent to the interface identified by this address.
- Multicast addresses: used to identify a group of interfaces, similar to the multicast addresses in IPv4. Datagrams sent to a multicast address will be sent to all interfaces identified by this address.
- Anycast addresses: used to identify a group of interfaces, a subgroup with an anycast address will

be only sent to an interface of that group. Depending on the routing protocol, the interface that receives the subgroup will be the interface that is closest to the source.

IPv6 address types are specified by the addresses' first few bits, which are referred to as format prefix. The correspondence between main address types and format prefixes is as shown in Table 1-2.

Table 34-2 Correspondence between IPv6 Address Types and Format Prefixes

Address type		Format prefix (binary)	Prefix identifier
Unicast address	Unspecified address	00...0 (128 bits)	::/128
	Loopback address	00...1 (128 bits)	::1/128
	Link local address	1111111010	FE80::/10
	Site local address	1111111011	FEC0::/10
	Global unicast address	Other formats	-
Multicast address		11111111	FF00::/8
Anycast address		An anycast address is designated from unicast address space and expressed in the format of unicast addresses	

There are multiple types of IPv6 unicast addresses, including global unicast addresses, link local addresses and site local addresses.

- Global unicast addresses are equivalent to IPv4 public addresses and are provided to Internet service providers. This type of address allows the aggregation of routing prefix, which limits the number of global routing table entries.
- Link local address is for neighbor discovery protocol and stateless autoconfiguration of communication between link local nodes. Datagrams with link local address as a source or destination address will not be forwarded to other links.
- Site-local addresses are equivalent to private IP addresses in IPv4. Datagrams with site local address as a source or destination address will not be forwarded to other sites beyond the local site.
- Loopback address: unicast address 0:0:0:0:0:0:0:1 (can be simplified as::1) is referred to as loopback address, which cannot be assigned to any physical interface. Its role is identical to the loop address in IPv4, that is, for a node to send IPv6 message to itself.
- Unspecified address: The address :: is referred to as unspecified address, which cannot be assigned to any node. Before acquiring a valid IPv6 address, a node fills this address in the source address

field of IPv6 messages. The unspecified address cannot be used as a destination IPv6 address.

IPv6 multicast addresses listed in Table 1-3 are reserved for special purposes.

Table 34-3 IPv6 Multicast Addresses Reserved for Special Purposes

Address	Application
FF01::1	Node-local scope all-nodes multicast address
FF02::1	Link-local scope all-nodes multicast address
FF01::2	Node-local scope all-routers multicast address
FF02::2	Link-local scope all-routers multicast address
FF05::2	Site-local scope all-routers multicast address

Configuration Conditions

None

Configure Interface IPv6 Address

Table 34-4 Configure Interface IPv6 Address

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure interface IPv6 address	**ipv6 address** { *linklocal-address* **link-local** | *prefix-address* [**anycast** | **eui-64**] | **autoconfig** }	Required By default, an interface is not configured an IPv6 address.

NOTE

- An interface can be configured multiple IPv6 addresses.

- After an interface is configured IPv6 address, it automatically enables IPv6 function.

34.2.2 Configure Basic Functions of IPv6 *-B -S -E -A*

Configuration Conditions

None

Turn on IPv6 Unicast Forwarding Function

By default, IPv6 unicast forwarding function is turned on. Under certain specific circumstances, the user can turn off IPv6 unicast forwarding function; once the function is turned off, IPv6 messages will not be forwarded.

Table 34-5 Turn on IPv6 Unicast Forwarding Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Turn on IPv6 unicast forwarding function	**ipv6 unicast-routing**	Required By default, IPv6 unicast forwarding function is turned on.

Turn on Interface IPv6 Function

Prior to the performance of IPv6 related configurations, IPv6 functions have to be turned on first, otherwise some configurations will not take effect.

Table 34-6 Turn on Interface IPv6 Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Turn on interface IPv6 function	**ipv6 enable**	Required By default, interface's IPv6 function is turned off

Configure IPv6 Message Hop Limit Value

IPv6 message header contains hop limit field, which serves a role identical to that of TTL field in IPv4 header, indicating the allowable forwarding times of the message in network by routers.

The hop limit value in IPv6 message header generated by the Device can be configured using a command.

Table 34-7 Configure IPv6 Message Hop Limit Value

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IPv6 message hop limit value	**ipv6 hop-limit** *value*	Required By default, the hop limit for IPv6 messages sent by Device is 64

Configure Interface's IPv6 MTU

Table 34-8 Configure Interface's IPv6 MTU

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure interface's IPv6 MTU	**ipv6 mtu** *value*	Required By default, interface's IPv6 MTU is not configured

34.2.3 Configure IPv6 Neighbor Discovery Protocol *-B -S -E -A*

IPv6 Neighbor discovery (ND) protocol includes the following functions: address resolution, neighbor unreachability detection, duplicate address detection, router discovery/prefix discovery, address autoconfiguration and redirect.

The types and roles of ICMPv6 message used by ND protocol are as shown in the following table.

Table 34-9 Types and Roles of ICMPv6 Messages Used in ND Protocol

ICMPv6 message type	Type No.	Role
Router Solicitation (RS) message	133	After initiation, a node send solicitation to router using RS message, requesting for a prefix and other configuration information for autoconfiguration of node
Router Advertisement(RA) message	134	Respond to RS message If RA message sending is not inhibited, router will periodically send RA messages, including prefix information option and some flag bit information
Neighbor Solicitation (NS) message	135	Get neighbor's link layer address Verify the reachability of neighbor Perform duplicate address detection
Neighbor Advertisement (NA) message	136	Respond to NS message When the link layer has changed, a node actively sends NA message to neighbor node to advertise its node change information.
Redirect message	137	When certain conditions are met, the default gateway sends redirect message to the source host so that the host can reselect correct next hop address for sending subsequent messages.

- Address resolution (ARP)

Get the link layer addresses of neighboring nodes in the same link via NS message and NA message.

- Neighbor unreachability detection

Upon the acquisition of the link layer addresses of neighboring nodes, the reachability of neighboring nodes can be verified by NS message and NA message.

1) A node sends NS message, the destination address of which is the neighboring node's IPv6 address.
2) If it receives acknowledge message from a neighboring node, then the neighboring node is deemed reachable; otherwise, the neighboring node is deemed unreachable.

- Duplicate address detection

When a node acquires IPv6 address, it has to use duplicate address detection function to verify whether the address has been used by another node.

- Router discovery/prefix discovery and address autoconfiguration

Router discovery/prefix discovery means a node gets the prefixes of its neighboring routers and their networks and other configuration parameters from the received RA message.

Stateless autoconfiguration of addresses means a node automatically configures IPv6 address according to information acquired through router discovery/prefix discovery.

Router discovery/prefix discovery is implemented by RS message and RA message.

- Redirect

When a host is started, its routing table may contain only one default route to the default gateway. When certain conditions are met, the default gateway will send ICMPv6 redirect message to the source host so that the host can select better next hop for sending subsequent messages.

Configuration Conditions

None

Configure IPv6 Static Neighbor

The resolution of neighboring nodes' IPv6 addresses to link layer addresses can be implemented with the ARP function in IPv6 ND protocol or by manually configuring static neighbors.

An IPv6 neighbor's sole identifier is its IPv6 address and the L3 interface connected to this neighboring node.

Table 34-10 Configure IPv6 Static Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IPv6 static neighbor	**ipv6 neighbor** *ipv6-address interface-name mac-address*	Required By default, IPv6 static neighbor is not configured

Configure the Aging Time of IPv6 Neighboring Table Entry in STALE Status

In IPv6 neighboring table entries, there are 5 reachability statuses: INCOMPLETE, REACHABLE, STALE, DELAY and PROBE. STALE status means the reachability of the neighbor is unknown, a neighboring table entry in STALE status has an aging time, when the aging time is expired, the neighboring table entries in STALE status will be migrated to DELAY status.

Table 34-11 Configure the Aging Time of IPv6 Neighboring Table Entry in STALE Status

Steps	Command	Description

Enter global configuration mode	**configure terminal**	-
Configure the aging time of IPv6 neighboring table entry in STALE status	**ipv6 neighbor stale-aging** *aging-time*	Optional By default, the aging time of IPv6 neighboring table entry in STALE status is 7200 seconds

Configure NS Message's Time Interval for Retransmission

After sending NS message, if Device does not receive response within the specified time interval, then it will resend the NS message. The following command can be used to configure the time interval for resending NS message.

Table 34-12 Configure NS Message's Time Interval for Retransmission

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure NS message's time interval for retransmission	**ipv6 nd ns-interval** *value*	Required By default, the time interval for interface to send NS message is 1000 milliseconds

Configure the Number of NS Messages Sent during IPv6 Duplicate Address Detection

After the configuration of IPv6 address, interface sends NS message to repeat address detection; if no response is received within a certain time period, it will continue to send NS message; when the number of sent NS messages reaches the set value without receiving any response, the address will be deemed usable.

Table 34-13 Configure the Number of NS Messages Sent during IPv6 Duplicate Address Detection

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-

Configure the number of NS messages sent during IPv6 duplicate address detection	**ipv6 nd dad attempts** *value*	Required By default, the transmission number of NS messages sent during IPv6 duplicate address detection is 1

Configure RA Message Related Parameters

The user may, depending on the actual situation, decide whether the interface will send RA message and configure the time interval for sending RA message; in the meantime, it can also configure relevant parameters in RA message and advertise them to the host. When receiving the RA message, the host can use these parameters for corresponding operations.

Table 34-14 Parameters in RA Messages and Their Descriptions

Parameter	Description
Hop Limit	When sending IPv6 message, the host will use the parameter values to fill the Hop Limit field of IPv6 message header. In the meantime, the parameter values can also serve as the Hop Limit field value in Device response message.
MTU	The sent link MTU can be used to ensure all nodes in the same link will use identical MTU value.
Router Lifetime	It is used to set a time period in which the RA message sending router serves as the host's default router. The host may, according to the router lifetime parameter value in the received RA message, decide whether or not to use the RA message sending router as the default router.
Reachable Time	When neighbor unreachability detection confirms the reachability of a neighbor, the Device will deem the neighbor as reachable within the set reachable time; beyond the set reachable time, if the host wants to send message to the neighbor, it will reverify whether the neighbor is reachable or not.

Table 34-15 Relevant Parameters of RA Messages

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Enter the interface configuration mode	**interface** *interface-name*	-
Configure the prefix option information in RA messages	**ipv6 nd prefix** { *ipv6-prefix* **| default** } [*valid-lifetime* **| infinite | no-advertise | no-autoconfig | off-link**] [*prefered-lifetime* **| infinite**]	Required By default, prefix option information in not configured.
The Hop Limit field value of the RA message sent by the configured interface is acquired from global configuration.	**ipv6 nd ra hop-limit**	Optional By default, the Hop Limit field value of the RA message sent by a not configured interface is acquired from global configuration, the Hop Limit field value is 0.
Configure the maximum time interval and minimum time interval for sending RA message	**ipv6 nd ra interval** *max-value* [*min-value*]	Optional By default, the maximum time interval for sending RA message is 600 seconds, the minimum time interval is 198 seconds
Configure the MTU option carried in RA message	**ipv6 nd ra mtu**	Optional By default, RA message does not carry MTU option
Configure router lifetime in RA message	**ipv6 nd ra-lifetime** *value*	Optional By default, router lifetime in RA message is 1800 seconds
Forbid interface to periodically send RA message	**ipv6 nd suppress-ra period**	Optional By default, interface will not periodically send RA message
Forbid interface to respond to RS message	**ipv6 nd suppress-ra response**	Optional By default, interface when receiving RS message will

		not respond to RA message

Turn on Interface Send Redirect Message Function

Upon receiving IPv6 message to be forwarded, if Device through routing discovers that the message's receiving interface is identical to the sending interface, it will forward the message and send back a redirect message to source to notify the source to reselect a correct next hop for the sending of subsequent messages. By default, the Device can send redirect message; under certain circumstances, however, the user may forbid the Device to send redirect message.

Table 34-16 Interface Send Redirect Message Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Turn on interface send redirect message function	**ipv6 redirects**	Optional By default, interface's sending redirect message function is turned on.

34.2.4 Configure ICMPv6 Function *-B -S -E -A*

In IPv6 protocol stacking, ICMP is mainly used to provide network detection service; when there is abnormality in network layer or transmission layer protocol, it provides error report and notifies corresponding Device to perform network control and management.

Configuration Conditions

None

Configure ICMPv6 Error Message Send Rate

If there are too many ICMPv6 error messages being sent in the network within a short period of time, network congestion may arise. In order to prevent this, user can configure the maximum number of ICMPv6 error messages sent within a specified period.

Table 34-17 ICMPv6 Error Message Send Rate

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure ICMPv6 message send rate	**ipv6 icmp error-interval** *interval* [*buckets*]	Optional

		By default, the cycle for calculating sending rate of ICMPv6 error messages is 100millisecond, and the maximum number of ICMPv6 error messages sent in a cycle is 10.

Turn on ICMPv6 Destination Unreachable Message Sending Function

ICMPv6 destination unreachable message sending function means that when Device receives IPv6 datagram, if the destination is unreachable, then the Device will discard the message and send ICMPv6 destination unreachable error message to the source.

When the following conditions are met, the Device will send ICMPv6 destination unreachable error message:

- When forwarding messages, if Device fails to find router, it will send ICMPv6 error message "no router reaching destination address" to source;
- When forwarding message, if it is unable to send message because of management strategy (e.g., firewalled, ACL, etc), the Device will send ICMPv6 error message "communication with destination address forbidden by management strategy" to source;
- When forwarding message, if the message's destination IPv6 address is beyond the range of source IPv6 address (e.g., message's source IPv6 address is link local address, message's destination IPv6 address is global unicast address), the message will not be able to reach destination, then Device will send ICMPv6 error message "beyond source address range" to source;
- When forwarding message, if the Device cannot resolve the link layer address corresponding to the destination IPv6 address, then it will send ICMPv6 error message "address unreachable" to source;
- When receiving IPv6 message with local destination address and UDP transmission layer protocol, if the message's destination port ID does not match the process in use, the Device will send ICMPv6 error message "port unreachable" to source.

When the information conveyed by ICMPv6 destination unreachable error message is unreachable information, if there is malicious attack, end user's normal use of Device may be affected. In order to prevent the above-mentioned phenomenon, the ICMPv6 destination unreachable error message sending function can be turned off.

Table 34-18 ICMPv6 Destination Unreachable Message Sending Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Turn on ICMPv6 destination unreachable message sending function	**ipv6 unreachables**	Optional By default, ICMPv6 destination unreachable message sending function is turned on

34.2.5 Configure IPv6 TCP Attack Defense Function *-B -S -E -A*

If IPv6 TCP server receives numerous SYN messages but the opposite end does not respond to the server's SYN+ACK reply. That will consume a lot of memory of the server and occupy the server's SYN queue, making the IPv6 TCP server unable to serve normal requests. This kind of attacks can be avoided by configuring IPv6 TCP attack defense function.

Configuration Conditions

None

Turn on IPv6 TCP syncache Function

When this function is enabled, the system does not rush to assign TCB upon receiving SYN datagram; instead, it replies a SYN ACK message first and saves the half-open connection information in a special cache and then assign TCB until it receives correct response ACK message.

Table 34-19 IPv6 TCP syncache Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Turn on IPv6 TCP syncache function	**ipv6 tcp syncache**	Required By default, IPv6 TCP syncache function is turned off

Turn on IPv6 TCP syncookies Function

This function uses no memory resources at all. Instead, it uses a special algorithm to generate a Sequence Number. The algorithm takes into account the opposite side's IPv6 address, port, oneself's IPv6 address, and port's fixed information, and oneself's information which the other side does not know and which is relatively invariable, such as MSS and time, and, upon receiving the other side's ACK message, recalculates the Sequence Number to see whether it is identical to the Sequence Number-1 in the other side's reply message, thereby deciding whether or not to assign TCB resources.

Table 34-20 IPv6 TCP syncookies Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Turn on IPv6 TCP syncookies function	**ipv6 tcp syncookies**	Required By default, IPv6 TCP syncookies function is turned off

34.2.6 Basic Monitoring and Maintenance of IPv6 *-B -S -E -A*

Table 34-21 Basic Monitoring and Maintenance of IPv6

Command	Description
clear ipv6 icmp6stat	Erase ICMPv6 statistical information
clear ipv6 interface statistics	Erase interface IPv6 message statistical information
clear ipv6 mtu	Erase IPv6 path MTU information
clear ipv6 neighbors	Erase IPv6 dynamic neighboring table entry
clear ipv6 statistics	Erase IPv6 base statistical information
clear ipv6 tcp syncache statistics	Erase IPv6 TCP protocol syncache statistical information
clear ipv6 tcp6stat	Erase IPv6 TCP statistical information
clear ipv6 udp6stat	Erase IPv6 UDP statistical information
show ipv6 hop-limit	Display IPv6 global Hop Limit value
show ipv6 frag-queue	Display cache's IPv6 fragment message
show ipv6 icmp6state	Display ICMPv6 statistical information
show ipv6 interface	Display interface IPv6 information
show ipv6 interface statistics	Display interface IPv6 statistical information
show ipv6 max-mtu	Display IPv6 MTU value currently supported by the system
show ipv6 mtu	Display IPv6 path MTU information
show ipv6 neighbors	Display IPv6 neighboring information
show ipv6 prefix	Display IPv6 address prefix information
show ipv6 sockets	Display IPv6 socket information

Command	Description
show ipv6 statistics	Display IPv6 base statistical information
show ipv6 tcp syncache detail	Display IPv6 TCP syncache table entry information
show ipv6 tcp syncache statistics	Display IPv6 TCP syncache statistical information
show ipv6 tcp6state	Display IPv6 TCP statistical information
show ipv6 udp6state	Display IPv6 UDP statistical information

34.3 Example of Basic Configuration of IPv6

34.3.1 Configure Interface IPv6 Address *-B -S -E -A*

Network Requirements

- Two devices are connected via ethernet interface and the interfaces are assigned IPv6 global unicast address for verifying their interoperability.

Network Topology

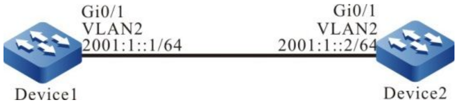


Figure 34-1 Networking Diagram - Configure Interface's IPv6 Address

Configuration steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Enable device's IPv6 forwarding capacity.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 unicast-routing
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 unicast-routing
```

Step 3: Configure interface's global unicast address.

#Configure Device1 interface vlan 2's global unicast address to 2001:1::1/64.

```
Device1(config)#interface vlan 2
```

```
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#exit
```

#Configure Device2 interface vlan 2's global unicast address to 2001:1::2/64.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#exit
```

Step 4: Check the result.

#Check Device1's interface information.

```
Device1#show ipv6 interface vlan 2
vlan2 is up
  VRF: global
  IPv6 is enable, link-local address is fe80::0201:7aff:fe46:a64d
  Global unicast address(es):
    2001:0001::0001, subnet is 2001:0001::/64
  Joined group address(es):
    ff02::0001:ff00:0001
    ff02::0001:ff00:0
    ff02::0002
    ff02::0001
    ff02::0001:ff46:a64d
  ND control flags: 0x1
  MTU is 1500 bytes
  ICMP redirects are enabled
  ICMP unreachables are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
```

After IPv6 address is configured, the interface will automatically enable IPv6 protocol function, automatically generate link local address, and join in corresponding multicast group.

#Check Device2's interface information.

```
Device2#show ipv6 interface vlan 2
vlan2 is up
  VRF: global
  IPv6 is enable, link-local address is fe80::0201:7aff:fe22:e222
  Global unicast address(es):
    2001:0001::0002, subnet is 2001:0001::/64
  Joined group address(es):
    ff02::0001:ff00:0002
  ff02::0001:ff00:0
  ff02::0002
  ff02::0001
  ff02::0001:ff22:e222
ND control flags: 0x1
MTU is 1500 bytes
ICMP redirects are enabled
ICMP unreachables are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
```

#On Device1, ping Device2's link local address fe80::0201:7aff:fe22:e222.

```
Device1#ping  fe80::0201:7aff:fe22:e222

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to fe80::201:7aff:fe22:e222 , timeout is 2 seconds:

Output Interface: vlan 2
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/96/483 ms.
```

NOTE

- When pinging link local address, it is necessary to specify the outgoing interface, which is an interface in the same link in which the pinged local address is located.

#On Device1, ping Device2's global unicast address 2001:1::2.

```
Device1#ping 2001:1::2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:1::2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/36/183 ms.
```

Device1 and Device2 should be able to communicate with each other.

34.3.2 Configure IPv6 Neighbor Discovery *-B -S -E -A*

Network Requirements

- Device and PC belong to the same LAN.
- Device's interface VLAN2 is configured EUI-64 address.
- PC acquires IPv6 address prefix through IPv6 neighbor discovery protocol and automatically configure IPv6 address according to the acquired address. IPv6 protocol based communication is implemented between PC and Device.

Network Topology

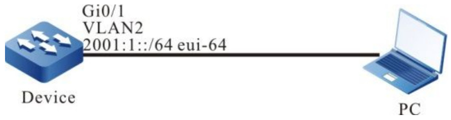


Figure 34-2 Networking Diagram - Configure IPv6 Neighbor Discovery

Configuration steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Enable device's IPv6 forwarding capacity.

```
Device#configure terminal
Device(config)#ipv6 unicast-routing
```

Step 3: Configure EUI-64unicast address, and enable RA advertisement function.

#Device's vlan 2 is configured EUI-64 address, and vlan 2's RA advertisement function is enabled.

```
Device(config)#interface vlan 2
Device(config-if-vlan 2)#ipv6 address 2001:1::/64 eui-64
Device(config-if-vlan 2)#no ipv6 nd suppress-ra period
Device(config-if-vlan 2)#no ipv6 nd suppress-ra response
Device(config-if-vlan 2)#exit
```

NOTE

- By default, RA advertisement function is turned off.

#Check Device's interface information.

```
Device#show ipv6 interface vlan 2
vlan2 is up
  VRF: global
  IPv6 is enable, link-local address is fe80::0201:7aff:fe5d:e7d3
```

```
Global unicast address(es):
  2001:0001::0201:7aff:fe5d:e7d3, subnet is 2001:0001::/64 [EUI]
Joined group address(es):
  ff02::0001:ff00:0
  ff02::0002
  ff02::0001
  ff02::0001:ff5d:e7d3
ND control flags: 0x85
MTU is 1500 bytes
ICMP redirects are enabled
ICMP unreachables are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
```

Step 4: Configure PC.

#Install IPv6 protocol on PC. IPv6 configuration varies depending on operating system. The example in this document is based on Windows XP.

```
C:\>ipv6 install
Installing...
Succeeded.
```

Step 5: Check the result.

#Check PC's interface information.

```
C:\>ipconfig
...(some displayed information is omitted here)
Ethernet adapter 130:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . . . . . . . . : 130.255.128.100
    Subnet Mask . . . . . . . . . . . : 255.255.0.0
    IP Address. . . . . . . . . . . . : 2001:1::15b3:d4:f13d:c3da
    IP Address. . . . . . . . . . . . : 2001:1::3a83:45ff:feef:c724
    IP Address. . . . . . . . . . . . : fe80::3a83:45ff:feef:c724%6
    Default Gateway . . . . . . . . . : fe80::201:7aff:fe5e:cfc1%6
```

It can be seen that the PC acquires IPv6 address prefix 2001:1::/64 and based on the prefix automatically generates global unicast address.

NOTE

- Upon acquisition of the address prefix, Windows XP host will generate two global unicast addresses. The interface ID of one address is generated in accordance with the interface's MAC address, the interface ID of another address is generated randomly.

#On the Device, ping PC's link local address fe80::3a83:45ff:feef:c724.

```
Device#ping fe80::3a83:45ff:feef:c724


Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to fe80::3a83:45ff:feef:c724 , timeout is 2 seconds:


Output Interface: vlan2

!!!!!

Success rate is 100% (5/5). Round-trip min/avg/max = 0/29/149 ms.
```

#On the Device, ping the global unicast addresses 2001:1::15b3:d4:f13d:c3da and 2001:1::3a83:45ff:feef:c724 automatically generated on PC.

```
Device#ping 2001:1::15b3:d4:f13d:c3da


Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to 2001:1::15b3:d4:f13d:c3da , timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5). Round-trip min/avg/max = 0/36/183 ms.


Device#ping 2001:1::3a83:45ff:feef:c724


Press key (ctrl + shift + 6) interrupt it.

Sending 5, 76-byte ICMP Echos to 2001:1::3a83:45ff:feef:c724 , timeout is 2 seconds:

!!!!!

Success rate is 100% (5/5). Round-trip min/avg/max = 0/26/133 ms.
```

PC and Device should be able to communicate with each other.

NOTE

- When pinging link local address, it is necessary to specify the outgoing interface, which is an interface in the same link in which the pinged local address is located.

35 DHCPv6

35.1 DHCPv6 Overview

A network can be hard to be managed when it is huge. For example, in a network environment where IPv6 addresses are manually assigned, the most common problem is IPv6 address conflict. The only method to solve this problem is to dynamically assign IPv6 address to the host. The Dynamic Host Configuration Protocol (DHCPv6) assigns IPv6 addresses from an address pool to requesting hosts. In the meantime, DHCPv6 can also provide other information, such as DNS server address. DHCPv6 reduces the burden on the administrator to track and record manually assigned IPv6 addresses.

DHCPv6 is a UDP broadcast based protocol. DHCPv6 client acquire IPv6 address and other configuration information from DHCPv6 server, the process mainly consists of four stages:

SOLICT stage: when DHCPv6 client logs in the network for the first time, it will send a DHCP SOLICT message to the network, the message's source address is the client's linklocal address and destination address is ff02::1:2;

ADVERTISE stage: when DHCPv6 server receives the DHCP SOLICT broadcast message sent by the client, it will select an IPv6 address from corresponding address pool in accordance with relevant strategy, the address and other parameters will be sent to the client through DHCP ADVERTISE message;

REQUEST stage: if DHCPv6 client receives responses from multiple DHCPv6 servers on the network, it will choose only one DHCP ADVERTISE (generally the first arrived one), and will send a DHCP REQUEST message to the network, telling all DHCPv6 servers the server from which it will receive the IPv6 address;

REPLY stage: when DHCPv6 server receives DHCPv6 client's DHCP REQUEST request message, it will send a DHCP REPLY acknowledgment information which contains the IPv6 address provided by it to the DHCPv6 client, telling the DHCPv6 client to use that IPv6 address.

The IPv6 address assigned by DHCPv6 server to DHCPv6 client has a lease period, upon expiry of which the DHCPv6 server will recover the assigned IPv6 address. When DHCPv6 client's IPv6 address's lease period has only one half remained, the DHCPv6 client will send a DHCP ENEW message to the DHCPv6 server for renewing its IPv6 lease period. If the DHCPv6 client can continue to use that IPv6 address, then the DHCPv6 server will reply a DHCP REPLY message, notifying the DHCPv6 client to renew the lease period; if the DHCPv6 client is not allowed to continue to use that IPv6 address, then the DHCPv6 server will not reply.

During the dynamic acquisition process of the IPv6 address, the request message is sent in multicast mode. Therefore, DHCPv6 is suitable only for circumstances in which the DHCPv6 client is in the same subnet with the DHCPv6 server. If there are multiple subnets in a network, and all hosts of multiple subnets needs the DHCPv6 server to provide configuration information such as IPv6 addresses, then these subnets' hosts can communicate with the DHCPv6 server via DHCPv6 relay devices, and will eventually acquire IPv6 addresses and other configuration information.

35.2 Configuration of DHCPv6 Function

Table 35-1 Functional Configuration List of DHCPv6

Configuration task	
Configure DHCPv6 address pool	Create DHCPv6 address pool, it is allowable to designate VRF attribute
	Configure IPv6 address range
	Configure DNS server address
	Configure IPv6 address lease period
	Configure IPv6 to bind with DUID, IAID
Configure DHCPv6 server's other parameters	Configure DHCPv6 server
	Configure reserved IPv6 address range
	Configure DHCPv6 ping detection parameters
	Configure DHCPv6 server's data journaling function
Configure DHCPv6 client function	Configure DHCPv6 client
	Configure DHCPv6 Option 16 function
Configure DHCPv6 relay function	Configure DHCPv6 relay
	Configure DHCPv6 relay message source address
	Configure DHCPv6 server address
	Configure DHCPv6 interface-id option

35.2.1 Configure DHCPv6 Address Pool *-S -E -A*

Configuration Conditions

None

Create DHCPv6 Address Pool

The DHCPv6 server chooses IPv6 addresses from the DHCPv6 address pool and assigns them and other relevant parameters to clients; as a result, the DHCPv6 server has to create the DHCPv6 address pool first.

Table 35-2 Create DHCPv6 Address Pool

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create DHCPv6 address pool and enter DHCPv6 configuration mode	**ipv6 dhcp pool** *pool-name***[vrf** *vrf-name* **]**	Required By default, the system does not create DHCPv6 address pool

NOTE

- There are two types of address pool, i.e., Network address pool and Range address pool, which can be configured with network and range commands, respectively.

Configure IPv6 Address Range

On DHCPv6 server, every DHCPv6 address pool should be configured corresponding IPv6 address ranges, in order to assign IPv6 addresses to DHCPv6 clients.

Table 35-3 Configure IPv6 Address Range

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter DHCPv6 configuration mode	**ipv6 dhcp pool** *pool-name***[vrf** *vrf-name* **]**	-
Configure Network type IPv6 address range	**network** *ipv6-address/prefix-length*	Optional By default, no IPv6 address range has been configured in address pool
Configure Range type IPv6 address range	**range** *low-ipv6-address high-ipv6-address prefix-length*	Optional By default, no IPv6 address range has been configured in address pool

NOTE

- Changing the type of an address pool from network to range (or from range to network): if newly configured address range intersects with originally configured address pool, the command line will prompt the user whether or not to execute the operation. If yes, relevant address configuration (static binding) and dynamic lease under the address pool will be deleted. If newly configured address' actual valid range contains originally configured address's actual valid range, relevant address configuration (static binding) under the address pool will be retained. However, dynamic lease will be deleted.

Configure DNS Server Address

On DHCPv6 server, you can configure DNS server address for every DHCPv6 address pool respectively. When assigning IPv6 address to DHCPv6 client, DHCPv6 server will also send the DNS server's address to the client.

When performing dynamic domain name resolution, DHCPv6 client will inquire the DNS server.

Table 35-4 Configure DNS Server Address

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter DHCPv6 configuration mode	**ipv6 dhcp pool** *pool-name***[vrf** *vrf-name* **]**	-
Configure DNS server address	**dns-server** { *ipv6-address*&<1-8> | **autoconfig** }	Required By default, DNS server address is not configured

Configure IPv6 Address Lease Period

The IPv6 address assigned by DHCPv6 server to the DHCPv6 client has a lease period, upon expiry of which the DHCPv6 server will recover the assigned IPv6 address. If DHCPv6 client wishes to continue to use that address, it has to renew the IPv6 address lease.

On DHCPv6 server, you can configure IPv6 address lease period for every DHCPv6 address pool separately.

Table 35-5 Configure Ipv6 Address Lease Period

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Enter DHCPv6 configuration mode	**ipv6 dhcp pool** *pool-name***[vrf** *vrf-name* **]**	-
Configure IPv6 address lease period	**lease preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*	Required By default, **preferred-lifetime** is 604800 seconds (7 days), **valid-lifetime** is 2592000 seconds (30 days)

Configure IPv6 to Bind with DUID, IAID

Configure IPv6 to bind with client DUID, IAID: when a client of designated DUID, IAID sends request to DHCPv6 server for the assignment of IPv6 address, the DHCPv6 server will assigned IPv6 address to be bound with the client. So long as the client's DUID, IAID remain unchanged, the client will get the same IPv6 address every time it requests for an address.

Table 35-6 Configure IPv6, DUID and IAID Address Binding

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter DHCPv6 configuration mode	**ipv6 dhcp pool** *pool-name***[vrf** *vrf-name* **]**	-
Configure IPv6 to bind with DUID, IAID	**bind** *ipv6-address* **duid** *duid* [**iaid** *iaid*]	Required By default, IPv6 DUID:IAID binding is not configured

NOTE

- The command only applies to Range type and Network type address pools.
- When identical duid and iaid static binding are configured, it is acceptable that an address pool is bound to five IPv6 addresses.
- If during the configuration of static binding only duid is specified and the iaid is not specified, the address pool is allowed to be bound to only one IPv6 address.

35.2.2 Configure DHCPv6 Server's Other Parameters *-S -E -A*

Configuration Conditions

None

Configure DHCPv6 Server

If interface is configured to work in DHCPv6 server mode, when the interface receives DHCPv6 request message sent by DHCPv6 client, the DHCPv6 server will assign IPv6 address and other network parameters to the client.

Table 35-7 Configure DHCPv6 Server

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure DHCPv6 server function	**ipv6 dhcp server**	Required By default, DHCPv6 server function is not configured

Configure Reserved IPv6 Address Range

In DHCPv6 address pool, some IPv6 addresses are reserved for certain devices. Some IPv6 addresses conflict with the IPv6 addresses of other hosts on the network, therefore, these IPv6 addresses cannot be used for dynamic assignation.

Table 35-8 Configure Reserved IPv6 Address Range

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure reserved IPv6 address range	**ipv6 dhcp excluded-address** *low-ipv6-address* [*high-ipv6-address*] [**vrf** *vrf-name*]	Required By default, reserved IPv6 address range is not configured IPv6 addresses within the reserved IPv6 address range do not participate in address assignation.

Configure DHCPv6 ping Detection Parameters

In order to prevent IPv6 address conflict, DHCPv6 server needs to test IPv6 address prior to dynamically assigning it to DHCPv6 client. The test is performed by pinging operation, the presence/absence of IPv6 address conflict is determined according to whether it can receive ICMPv6 echo response message within the specified time.

Table 35-9 Configure DHCPv6 ping Detection Parameters

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure DHCPv6 ping detection parameters	**ipv6 dhcp ping** { **packets** *packet-num* | **timeout** *milliseconds* }	Required By default, the number of ping packet is 1, time-out is 500ms

Configure DHCPv6 Server Data Journaling Function

After DHCPv6 server's data journaling function is turned on, the assignation of address pool on DHCPv6 server will be recorded into data log.

Table 35-10 Configure DHCPv6 Server Data Journaling Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure DHCPv6 server's data journaling function's turn on/off	**ipv6 dhcp logging security-data**	Required By default, data journaling function is not turned on

35.2.3 Configure DHCPv6 Client Function *-S -E -A*

Configuration Conditions

None

Configure DHCPv6 Client

DHCPv6 client interface can get IPv6 address and other parameters via DHCPv6.

Table 35-11 Configure DHCPv6 Client

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-

Configure DHCPv6 client to get IPv6 address	**ipv6 dhcp client address [rapid-commit]**	Required By default, DHCPv6 client is not configured to request for IPv6 address
Configure DHCPv6 client to get IPv6 prefix	**ipv6 dhcp client pd** *pool-name* **[rapid-commit]**	Required By default, DHCPv6 client is not configured to request or IPv6 prefix

35.2.4 Configure DHCPv6 Relay Function *-S -E -A*

Configuration Conditions

None

Configure DHCPv6 Relay

If there are multiple subnets in a network, and all hosts of multiple subnets needs the DHCPv6 server to provide configuration information such as IPv6 addresses, then these subnets' hosts can communicate with the DHCPv6 server via DHCPv6 relay devices, and will eventually acquire IPv6 addresses and other configuration information. If interface is configured to work in DHCPv6 relay mode, when the interface receives DHCPv6 message sent by DHCPv6 client, it will relay the message to the configured DHCPv6 server, the DHCPv6 server will assign the IPv6 address.

Table 35-12 Configure DHCPv6 Relay

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure DHCPv6 relay function	**ipv6 dhcp relay**	Required By default, DHCPv6 relay function is not configured

Configure DHCPv6 Relay Message Source Address

When DHCPv6 relaying the source address of message from DHCPv6 client to servers, by default it will use the routing outgoing interface address to DHCPv6 server; under certain special circumstances, DHCPv6 server is unable to communicate with that address. In such cases, the user is allowed to use **ipv6 dhcp relay source-address** command to configure the source address and the LinkAddr field of the message to be relayed to DHCPv6 server by DHCPv6;

Table 35-13 Configure DHCPv6 Relay Message Source Address

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure DHCPv6 relay message source address	**ipv6 dhcp relay source-address** *ipv6-address*	Required By default, DHCPv6 relay message source address is not configured

Configure DHCPv6 Server Address

When the interface receives DHCPv6 message sent by DHCPv6 client, it will relay the message to the configured DHCPv6 server, the DHCPv6 server will assign the IPv6 address.

Table 35-14 Configure DHCPv6 Server Address

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure DHCPv6 server address	**ipv6 dhcp relay server -address** *ipv6-address*	Required By default, DHCPv6 server address is not configured

Configure DHCPv6 Interface-id Option

The command is used to configure the interface-id option filling mode supported by DHCPv6 relays.

Table 35-15 Configure DHCPv6 Server Address

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure DHCPv6 interface-id option	**ipv6 dhcp relay interface –id [interface]**	Required

		By default, interface-id option filling mode is not configured

35.2.5 DHCPv6 Monitoring and Maintenance *-S -E -A*

Table 35-16 DHCPv6 Monitoring and Maintenance

Command	Description
clear ipv6 dhcp pool *pool-name* { **lease** | **conflict [***ipv6-address***]** }	Erase the dynamic lease information or address conflict information in address pool
clear ipv6 dhcp server interface [*interface-name* **] statistics**	Erase key information statistics of message interaction between DHCPv6 server and client or relay
clear ipv6 dhcp relay statistics	Erase statistical information on DHCPv6 relay device
show ipv6 dhcp server interface *interface-name* **[statistics]**	Display the address pool information associated with designated interface or display key information statistics of message interaction on designated interface between DHCPv6 server and client or relay
show ipv6 dhcp pool *pool-name* **{ summary | ping_list | offer_list | excluded_list | conflict_list | lease | binding }**	Display summary information of designated address pool or information of address being pinged or OFFER message that has been sent, wait for address information of DHCPv6 client's response to REQUEST message, or display address information having been excluded from address pool, or display information of addresses in address pool that has address conflict, or display dynamic lease information in address pool, or display static binding information in address pool.

show ipv6 dhcp pool *pool-name* **specific { ipv6-address** *ipv6-address* **| duid** *duid* **}**	Display information related to designated ip addresses in address pool or client's DUID.
show ipv6 dhcp relay [interface *interface-name* **]**	Display DHCPv6 relay device's message statistical information.

35.3 Example of DHCPv6 Typical Configuration

35.3.1 Static Assignation of IPv6 Addresses *-S -E -A*

Network Requirements

- Device2 serves as DHCPv6 server, and operates in static mode to assign client IPv6 address and DNS server IPv6 address.
- DHCPv6 server assigns IPv6 address to PC1 in DUID binding mode, and assigns IPv6 address to PC2 in DUID+IAID binding mode.

Network Topology

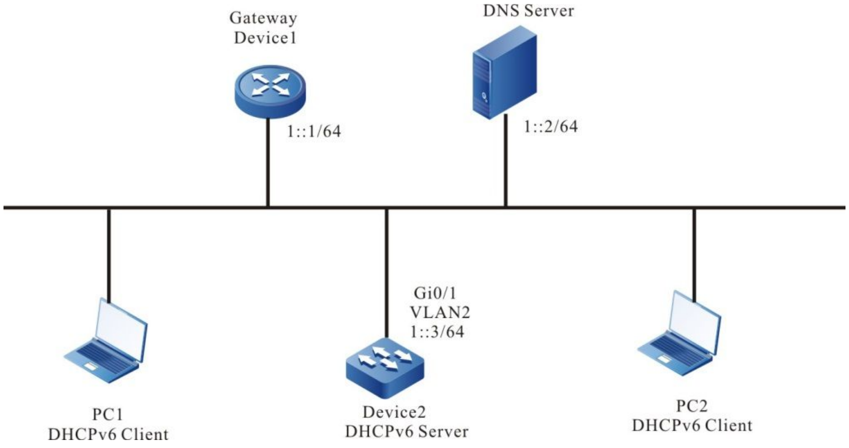


Figure 35-1 Networking Diagram - Static Assignation of IPv6 Addresses

Configuration Steps

Step 1: Configure Device2 interface's IPv6 address and DHCPv6 server.

```
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address 1::3/64
Device2(config-if-vlan2)#ipv6 dhcp server
Device2(config-if-vlan2)#exit
```

Step 2: Configure static binding address pool and parameter.

#Configure address pool binding, use static DUID binding to assign IPv6 address to PC1. Assign IPv6 address to PC2 by DUID+IAID binding

```
Device2(config)#ipv6 dhcp pool binding

Device2(dhcp6-config)#bind 1::11 duid 000200001613303030313761636635646634

Device2(dhcp6-config)#bind 1::12 duid 000200001613636364383166313037616239 iaid 00010071

Device2(dhcp6-config)#dns-server 1::2

Device2(dhcp6-config)#exit
```

Step 3: Check the result.

#Check the association of server interfaces with addresses

```
Device2#show ipv6 dhcp server interface vlan2

DHCPv6 server status information:

DHCP server is enabled on interface: vlan2

Vrf : global


DHCPv6 server pool information:

Available directly-connected pool:

     Interface IP: 1::1/64

       Pool name: binding

       Range:

           min: 101::

           max: 101::ffff:ffff:ffff:ffff

        utilization: 0.00%
```

#Check server's static binding

```
Device2#show ipv6 dhcp pool binding binding

IPv6 Address          Duid                          Iaid      Type    Time Left(s)

------------  -----------------------------------       --------   -------  ------------

     1::11       000200001613303030313761636635646634    00000000   Binding      NA

     1::12       000200001613636364383166313037616239    00010071   Binding      NA
```

#On Device2, use ipv6 dhcp pool binding lease command to check the IPv6 addresses assigned to PC1, PC2.

```
Device2#show ipv6 dhcp pool mac-binding lease

IPv6 Address           Duid                         Iaid      Type      Time Left(s) ------------  -----------------------
------------       --------   -------   ------------

1::11        000200001613303030313761636635646634        00000000    Lease       2591974

1::12        000200001613636364383166313037616239        00010071    Lease       2591974
```

On PC1 and PC2, check the correctness of the acquired IPv6 addresses, DNS server IPv6 address.

35.3.2 Dynamic Assignation of IPv6 Addresses *-S -E -A*

Network Requirements

- Configure IPv6 addresses 1::3/64 and 2::3/64 to Device's two interfaces vlan2, vlan3 respectively.
- DHCPv6 server device dynamically assigns IPv6 addresses in 1::/64 and 2::/64 network segments to clients in two directly connected physical networks.
- The lease period is 1 day for addresses in network segment 1::/64, DNS server address is 2::4; 3 days for addresses in network segment 2::/64, gateway address is 2::3, DNS server address is 2::4.
- Network segment1::/64 and the first 10 IPv6 addresses in network segment 2::/64 are reserved.

Network Topology

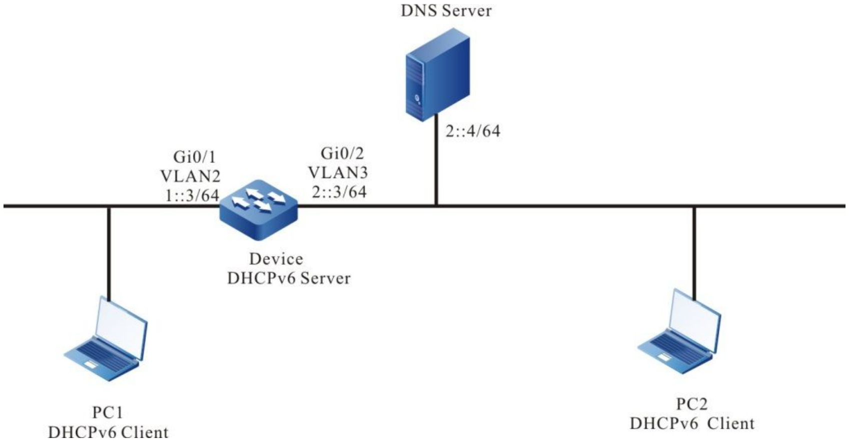


Figure 35-2 Networking Diagram - Dynamic Assignation of IPv6 Address

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. Configure IPv6 addresses of the interfaces (omitted)

Step 2: On DHCPv6 server Device1, configure 2 dynamic address pools and their parameters.

#Configure DHCPv6 server

```
Device(config)#interface vlan2
Device(config-if-vlan2)#ipv6 dhcp server
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 dhcp server
Device(config-if-vlan3)#exit
```

#Configure to reserve the first 10 IPv6 addresses in two address pools

```
Device(config)#ipv6 dhcp excluded-address 1::0 1::9
Device(config)#ipv6 dhcp excluded-address 2::0 2::9
```

#Configure the address pool named dynamic-pool1 and its parameters (address range, dns address, address lease period).

```
Device(config)#ipv6 dhcp pool dynamic-pool1

Device(dhcp6-config)#network 1::/64

Device(dhcp6-config)#dns-server 2::4

Device(dhcp6-config)#lease preferred-lifetime 86300 valid-lifetime 86400

Device(dhcp6-config)#exit
```

#Configure the address pool named dynamic-pool2 and its parameters (address range, dns address, address lease period).

```
Device(config)#ip DHCPv6 pool dynamic-pool2

Device(dhcp6-config)#network 2::/64

Device(dhcp6-config)#dns-server 2::4

Device(dhcp6-config)#lease preferred-lifetime 259100 valid-lifetime 259200

Device(dhcp6-config)#exit
```

Step 3: Check the result.

#Check the information of IPv6 addresses assigned to client on Device.

```
Device#show ipv6 dhcp pool dynamic-pool1 lease

IPv6 Address          Duid                        Iaid     Type      Time Left(s)

------------     --------------------------     --------  -------    ------------

1::a         00020000161330303031376163663564634   00000000   Lease       86390

Device2#show ipv6 dhcp pool dynamic-pool2 lease

IPv6 Address       Duid                     Iaid        Type      Time Left(s)

------------    ------------------------     --------     -------     ------------

2::a       00020000161330303031376163663564634  00000000    Lease       2591974
```

On DHCPv6 client, check the correctness of the acquired IPv6 addresses.

NOTE

- IPv6 addresses in the address pool must be in the network segment range of the interface that provides service.

35.3.3 Configure DHCPv6 Relay *-S -E -A*

Network Requirements

- Device1 serves as DHCPv6 server, Device2 interface has DHCPv6 relay function enabled.
- DHCPv6 server provides service to clients in network segment 1::/64, the first 10 IPv6 addresses are reserved.

- DHCPv6 client acquires IPv6 address via DHCPv6 relay.

Network Topology

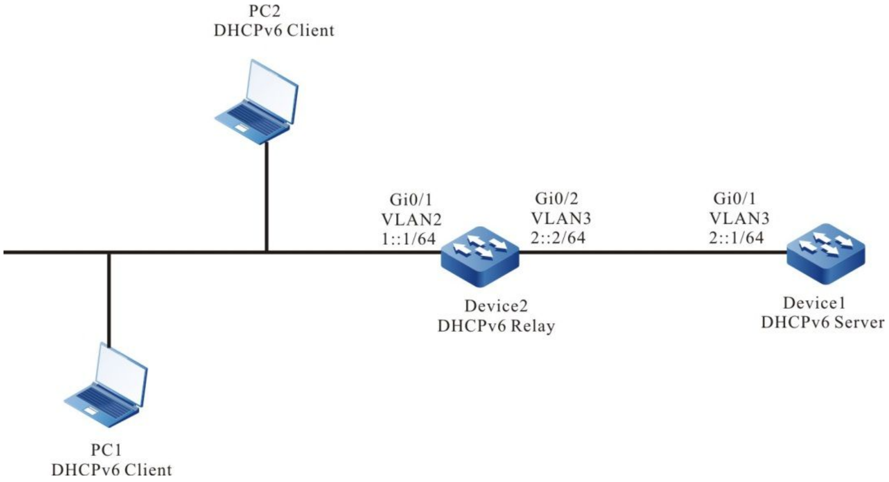


Figure 35-3 Networking Diagram - Configure DHCPv6 Relay

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. Configure IPv6 addresses of the interfaces (omitted).

Step 2: Configure Device1 IPv6 address pool and reserved IPv6 addresses.

#Configure Device1 as DHCPv6 server.

```
Device1#configure terminal
Device1(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 dhcp server
Device2(config-if-vlan3)#exit
```

#Configure to reserve IPv6 addresses 1::0 to 1::9.

```
Device1(config)#ipv6 dhcp excluded-address 1::0 1::9
```

#Configure Device1 IPv6 address pool dynamic-pool.

```
Device1(config)#ipv6 dhcp pool dynamic-pool
Device1(dhcp6-config)#network 1::/64
Device1(dhcp6-config)#lease preferred-lifetime 300 valid-lifetime 600
Device1(dhcp6-config)#exit
```

#Configure static routing to network segment 1::/64.

```
Device1(config)#ipv6 route 1::0/64 2::2
```

Step 3: On vlan2 interface of Device2, turn on DHCPv6 relay and configure DHCPv6 server address 2::1.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 dhcp relay
Device2(config-if-vlan2)#ipv6 dhcp relay server-address 2::1
```

```
Device2(config-if-vlan2)#exit
```

Check the result.

Step 4: #Check the information of IPv6 addresses assigned to Device1.

```
Device1#show ipv6 dhcp pool dynamic-pool lease
IPv6 Address            Duid                          Iaid      Type     Time Left(s)
------------   ----------------------------------      --------  -------    ------------
1::0          00020000161330303031376163663564663 4        00000000    Lease       574
```

Use show ipv6 dhcp pool dynamic-pool lease command to check the information of IPv6 address assigned to client, verifying that IPv6 address1::0 has been acquired by client

36 Routing Basics

36.1 Overview

After a device receives a packet through an interface, the device selects a route according to the destination of the route and then forwards the packet to another interface. This process is called routing. In network devices, routes are stored in a routing table database. The packets search the routing table to determine the next hop and output interface according to the destination of the packets. Routes are categorized into three types according to their sources.

- Direct route: The route is generated based on the interface address. After a user configures the IP address of an interface, the device generates a direct route of the network segment according to the IP address and mask.
- Static route: The route is manually configured by the user.
- Dynamic route: The route is discovered through the dynamic route discovery protocol. Based on whether the dynamic routing protocol is used within an autonomous domain, two types of dynamic routing protocols are available: Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP). Here an autonomous domain refers to a network which has a unified management organization and unified route policy. A routing protocol that is used within an autonomous domain is an IGP. Common IGPs include Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). EGPs are usually used for routing among multiple autonomous domains. A common EGP is BGP.

Routing supports load balancing, that is, multiple routes to the same destination. In forwarding packets, a device transmits packets in load balancing mode according to the routing table search result.

36.2 Routing Basic Function Configuration

Table 36-1 Routing Basic Function List

Configuration Tasks	
Configure load balancing for routing.	Configure the maximum number of load balancing entries.
Configure the capacity of routes for Virtual Route Forwarding (VRF) routes.	Configure the capacity of VRF routes.

36.2.1 Configure Load Balancing for Routing *-B -S -E -A*

Configuration Conditions

None

Configure the Maximum Number of Load Balancing Entries

If the costs of several paths to one destination are the same, the paths form load balancing. Configuring the maximum number of load balancing entries helps to improve the link utility rate and reduce the load of links.

Table 36-2 Configuring the Maximum Number of Load Balancing Entries

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the maximum number of load balancing entries.	**route path-limit** *max-number*	Optional. By default, the maximum number of load balancing entries for routing is 4.

36.2.2 Configure the Capacity of VRF Routes *-E -A*

Configuration Conditions

None

Configure the Capacity of VRF Routes

To ensure normal use of devices and prevents a large number of routes from consuming too many resources, you can use the **routing-table limit** command to limit the capacity of routes for each Virtual Route Forwarding (VRF). When the capacity of routes reaches the threshold, an alarm is generated.

Table 36-3 Configuring the Capacity of VRF Routes

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the VRF configuration mode.	**ip vrf** *vrf-name*	-

Step	Command	Description
Configure the capacity of VRF routes.	**routing-table limit** *limit-value* { *threshold-value* | **syslog-alert** }	Optional. By default, the capacity for routes is 55000. When the number of routes reaches 80% of the total capacity, alarm information is printed.

NOTE

- This command cannot limit the capacity of routes for global VRF.
- If the number of routing entries exceeds the threshold, new routing information gets lost.
- For VRF-related configuration, refer to the *MPLS L3VPN Configuration Manual*.

36.2.3 Routing Basics Monitoring and Maintaining *-B -S -E -A*

Table 36-4 Routing Basics Monitoring and Maintaining

Command	Description
clear ip route [**vrf** *vrf-name*] { *ip-address mask* **| all** }	Clears the specified IP route in the routing table.
show ip route [**vrf** *vrf-name*] [**bgp | connected | irmp | isis | ospf | rip | static | statistic** [**all**] | *ip-address* { *mask* | *mask-len* }]	Display IP route information.

37 IPv6 Routing Basics

37.1 Overview

After a device receives an IPv6 packet through an interface, the device selects a route according to the destination of the IPv6 packet and then forwards the packet to another interface. This process is called routing. In network devices, routes are stored in a routing table database. The packets search the routing table to determine the next hop and output interface according to the destination of the packets. Routes are categorized into three types according to their sources.

- Direct route: The route is generated based on the interface address. After a user configures the IPv6 address of an interface, the device generates a direct route of the network segment according to the address and mask.
- Static route: The route is manually configured by the user.
- Dynamic route: The route is discovered through the dynamic route discovery protocol. Based on whether the dynamic routing protocol is used within an autonomous domain, two types of dynamic routing protocols are available: Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP). Here an autonomous domain refers to a network which has a unified management organization and unified route policy. A routing protocol that is used within an autonomous domain is an IGP. Common IGPs include RIPng and OSPFv6. EGPs are usually used for routing among multiple autonomous domains. A common EGP is IPv6 BGP.

Routing supports load balancing, that is, multiple routes to the same destination. In forwarding packets, a device transmits packets in load balancing mode according to the routing table search result.

37.2 IPv6 Routing Basic Function Configuration

Table 37-1 IPv6 Routing Basic Function List

Configuration task	
Configure load balancing for IPv6 routing	Configure the maximum number of IPv6 load balancing entries
	Configure IPv6 load balancing calculations

37.2.1 Configure Load Balancing for IPv6 Routing *-B -S -E -A*

Configuration Conditions

None

Configure IPv6 load balancing calculations

There are three calculation methods for load balancing as follows:

- Calculation based on source and destination addresses: the source address and destination address are used to identify a stream, and the packets of the same stream take the same path without being out of order. Load unbalancing of the streams may result in the line load unbalancing.
- Calculation based on source address: use only the source address to identify a stream. The packets of the same stream use the same path to ensure that the same stream along the same path will not be out of order. Load unbalancing of the streams may result in the line load unbalancing.
- Calculation based on packets: packets to the same destination take different paths to achieve the load balance on each path, but may be out of order.

Table 37-2 Configure IPv6 Load Balancing Calculations

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IPv6 load balancing calculations	**ipv6 load-sharing** { **per-destination** | **per-packet** | **per-source** }	Optional By default, calculation based on source and destination addresses is used

37.2.2 IPv6 Routing Basics Monitoring and Maintaining *-B -S -E -A*

Table 37-3 IPv6 Routing Basics Monitoring and Maintaining

Command	Description
clear ipv6 route { *ipv6-address* **|** *ipv6-prefix* **| all** }	Clear the specified IPv6 route in the routing table
show ipv6 route [**vrf** *vrf-name*] [*ipv6-address* | *ipv6-prefix* | **bgp** | **brief** | **connected** | **isis** | **linklocal** | **local** | **ospf** | **rip** | **static** | **statistic** | **all**]	Display IPv6 route information

38 Static Routes

38.1 Overview

A static route is a self-defined route which is manually configured by a user. It specifies a path for transmitting IP packets which are targeted at a specified destination.

Compared with dynamic routing, static routing has higher security and lower device resource occupancy. The disadvantage is that when the network topology changes, manual configuration is required, and there is no automatic re-configuration mechanism.

Static routes do not occupy line bandwidth or occupy CPU to calculate and advertise routes periodically, improving the device and network performance.

Static routes can be used to ensure the security of a small-scale network, for example, in a network where there is only one path connecting to an external network. In a large-scale network, static routes can implement security control on services or links of certain types. A majority of networks adopt dynamic routing protocols but you can still configure some static routes for special purposes.

Static routes can be re-distributed to a dynamic routing protocol, but dynamic routes cannot be re-distributed to static routes. Note that improper static route configuration may cause routing loops.

The default route is a special route which can be a static route. In a routing table, the default route is a route to network 0.0.0.0 with the mask 0.0.0.0. You can use the **show ip route** command to check whether the route is valid. When the destination address of a received packet does not match any entry in the routing table, the packet takes the default route. If no default route is available and the destination is not in the routing table, the packet is discarded, and an ICMP packet is returned to the source end reporting that the destination address or network is not reachable. To prevent the routing table from becoming too large, you can set a default route. The packet that fails to find a matching routing table entry takes the default route for forwarding.

38.2 Static Routing Function Configuration

Table 38-1 Static Route Configuration Function List

Configuration Tasks	
Configure a static route.	Configure a static route.
Configure the default administrative distance.	Configure the default administrative distance.
Configure the recursive function.	Configure the recursive function.
Configure load balancing routes.	Configure load balancing routes.

Configuration Tasks	
Configure a floating route.	Configure a floating route.
Configure a static route to link with Track.	Configure a static route to link with Track.

38.2.1 Configure a Static Route *-B -S -E -A*

Configuration Conditions

Before configuring a static route, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.

Configure a Static Route

According to the parameters that have been specified, static routes are categorized into the following three types:

- Interface route: For an interface route, only the output interface is specified.
- Gateway route: For a gateway route, only the gateway address is specified.
- Interface gateway route: For an interface gateway route, both the output interface and the gateway address are specified.

Configured static routes become invalid if some of the following conditions are met:

1) The destination address is the local interface address.
2) The destination address is the network of the local direct interface.
3) The administrative distance of the route is 255.
4) The output interface of the route is DOWN.
5) No IP address has been configured for the output interface of the route.
6) The gateway address is not reachable.
7) The output interface and the gateway of the route conflict.
8) The output interface of the route does not exist.
9) The TRACK object that is associated with the route is "fake".
10) The status of the Bidirectional Forwarding Detection (BFD) session that is associated with the route is DOWN.

If an interface route meets any one condition among 1, 2, 3, 4, 5, 9, and 10, the route is invalid. If a gateway route meets any one condition among 1, 2, 3, 4, 6, 8, 9, and 10, the route is invalid. If an interface gateway route meets any of the above conditions, the route is invalid.

Table 38-2 Configuring a Static Route

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure a static route.	**ip route** [**vrf** *vrf-name1*] *destination-ip-address destination-mask* { *interface-name* / [*nexthop-ip-address* [**vrf** *vrf-name2*]] } [**name** *nexthop-name*] [**tag** *tag-value*] [**track** *track-id*] [*administrative-distance*]	Mandatory. The field *administrative-distance* is the administrative distance of the static route. If it is not specified, the default administrative distance is used.

NOTE

- For a default route, the destination network and mask must be set to 0.0.0.0.
- The output interface of the Null0 route is Null0.
- The output interface of the Null0 interface need not be configured with an IP address.

38.2.2 Configure the Default Administrative Distance *-B -S -E -A*

Configuration Conditions

None

Configure the Default Administrative Distance

The smaller the administrative distance that is specified for a static route in configuring the static route is, the higher the priority of the route is. If the administrative distance is not specified, the default administrative distance is used. You can modify the default administrative distance dynamically. After the default administrative distance is re-configured, the new default administrative distance is valid only for new static routes.

Table 38-3 Configuring the Default Administrative Distance

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enters the static route configuration mode.	**router static**	-

Step	Command	Description
Configure the default administrative distance.	**distance** *administration-distance*	Optional. The default value of the default administrative distance is 1.

NOTE

- When you use the **ip route** command to configure a static route, you can specify an independent administrative distance for the route. If you do not specify the administrative distance, the default administrative distance is used.

38.2.3 Configure the Recursive Function *-B -S -E -A*

Configuration Conditions

None

Configure the Recursive Function

If the gateway address that is configured for a route is valid only when a route to the gateway is reachable, you must enable the recursive function of the static route to validate the route. By default, the recursive function is enabled for a static route.

Table 38-4 Configure the Recursive Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enters the static route configuration mode.	**router static**	-
Configure a static route to support the recursive function.	**recursion**	Optional. By default, a static route supports the recursive function for routing.

38.2.4 Configure Load Balancing Routes *-B -S -E -A*

Configuration Conditions

None

Configure Load Balancing Routes

Load balancing routes means that multiple routes are configured to the same destination network. The output interfaces and the gateway addresses of the routes are different, but the administrative distances (priorities) of the routes are the same. Load balancing routes help to improve the link utility rate.

Table 38-5 Configuring Load Balancing Routes

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the first load balancing route.	**ip route** *destination-ip-address destination-mask interface-name1 distance*	Mandatory. The output interface is interface-name1.
Configure the second load balancing route.	**ip route** *destination-ip-address destination-mask interface-name2 distance*	Mandatory. The output interface is interface-name2.

NOTE

- In configuring load balancing routes, you must configure the values of distance for the routes to the same.

38.2.5 Configure a Floating Route *-B -S -E -A*

Configuration Conditions

None

Configure a Floating Route

Multiple routes are available to the same destination network. The output interfaces or gateway addresses of the routes are different, and the priorities of the routes are also different. The route with the higher priority becomes the primary route while the route with the lower priority becomes the floating route. In the routing table, only the primary route is visible. The floating table appears in the routing table only when the primary route becomes invalid. Therefore, the floating route is usually used as a backup route.

Table 38-6 Configuring a Floating Route

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the primary route.	**ip route** *destination-ip-address destination-mask interface-name1 distance1*	Mandatory. The output interface of the primary route is *interface-name1* and the priority of the route is *distance1*.
Configure the floating route.	**ip route** *destination-ip-address destination-mask interface-name2 distance2*	Mandatory. The output interface of the floating route is *interface-name2*, the priority is *distance2*. The value of *distance2* must be larger than the value of *distance1*.

NOTE

- In configuring the priorities of the routes, not that the smaller the *distance* value is, the higher the priority is.

38.2.6 Configure a Static Route to Link with BFD *-E -A*

Configuration Conditions

None

Configure a Static Route to Link with BFD

BFD (Bidirectional Forwarding Detection) protocol provides a method to detect the connected state of forwarding path between two adjacent routers quickly and under light load. In this way, the protocol neighbor can quickly detect the connecting fault of the forwarding path. Unlike other dynamic protocol routes, the static route cannot perceive the faults in the communication link. BFD provides a method to detect the faults of communication link quickly for static route, and the switching of routes can be realized quickly after configuring a static route to link with BFD. At present, the static route only supports the establishment of asynchronous BFD detection mode, so it is necessary to configure the static routes on devices at both ends of the link to link with BFD.

When the associated BFD state of the static route is DOWN, the configured static route will fail.

Table 38-7 Configuring a Static Route to Link with BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure a static route	**ip route** *destination-ip-address destination-mask interface-name nexthop-ip-address*	Required Only a static route that specifies both the output interface and the gateway address can link with BFD
Configure the output interface and next hop address of the route associated with the BFD	**ip route static bfd** *interface-name nexthop-ip-address*	Required *nexthop-ip-address* is the next hop address of direct route

NOTE

- Refer to bfd configuration manual for the introduction and basic function configuration of bfd;

38.2.7 Configure a Static Route to Link with Track *-B -S -E -A*

Configuration Conditions

None

Configure a Static Route to Link with Track

Some modules in the system need to monitor some system information and then determine their working modes based on the information. The objects that are monitored by the other modules are called monitoring objects. To simplify the relations between the modules and monitoring objects, Track objects are used. A Track object can contain multiple monitoring objects, and it displays the comprehensive status of the monitoring object to external modules. The external modules are associated only with Track objects and they do not care about monitoring objects contained in the Track objects any more. A Track object has two statuses, "true" and "false". The external modules that are associated with the Track object determine its working modes according to the Track object status.

A static route can associate with a Track object to monitor system information and determine whether the route is valid according to the status reported by the Track object. If the Track object reports "true", the conditions required by the static route are satisfied, and the route is added to the routing table. If the Track object reports "false", the route is deleted from the routing table.

Table 38-8 Configuring a Static Route to Link with Track

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create a Track object and enter the configuration mode of the Track object.	**track** *track-id*	Mandatory.
Configure the track object to monitor the link status of the specified interface.	**interface** *interface-name* **line-protocol**	Optional.
Return to the global configuration mode.	**exit**	-
Configure a static route and associate it with the Track object.	**ip route** *destination-ip-address destination-mask interface-name* **track** *track-id*	Mandatory. When the link layer of the monitoring interface is UP, the route is valid; otherwise, the route is invalid.

38.2.8 Static Route Monitoring and Maintaining *-B -S -E -A*

Table 38-9 Static Route Monitoring and Maintaining

Command	Description
show ip route [**vrf** *vrf-name*] **static**	Display the static routes in the routing table.
show running-config ip route	Display the configuration information about static routes.

38.3 Typical Configuration Example of Static Routes

38.3.1 Configure Static Routing Basic Functions *-B -S -E -A*

Network Requirement

- On Device1, Device2 and Device3, configure static routes so that PC1 and PC2 can communicate with each other.

Network Topology

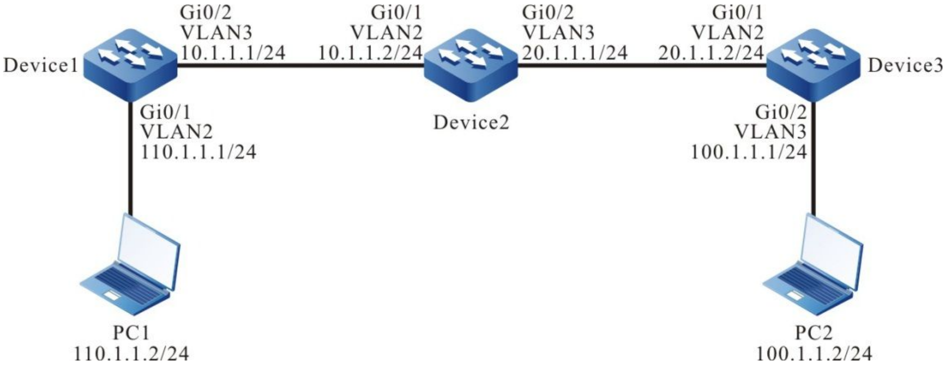


Figure 38-1 Networking for Configure Static Routing Basic Functions

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure static routes.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ip route 20.1.1.0 255.255.255.0 10.1.1.2
Device1(config)#ip route 100.1.1.0 255.255.255.0 10.1.1.2
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ip route 110.1.1.0 255.255.255.0 10.1.1.1
Device2(config)#ip route 100.1.1.0 255.255.255.0 20.1.1.2
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ip route 0.0.0.0 0.0.0.0 20.1.1.1
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 00:06:47, vlan3
S   20.1.1.0/24 [1/100] via 10.1.1.2, 00:00:13, vlan3
S   100.1.1.0/24 [1/100] via 10.1.1.2, 00:00:05, vlan3
C   110.1.1.0/24 is directly connected, 00:08:21, vlan2
C   127.0.0.0/8 is directly connected, 28:48:33, lo0
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

```
C   10.1.1.0/24 is directly connected, 00:00:37, vlan2
C   20.1.1.0/24 is directly connected, 00:00:27, vlan3
S   100.1.1.0/24 [1/100] via 20.1.1.2, 00:00:05, vlan3
S   110.1.1.0/24 [1/100] via 10.1.1.1, 00:00:13, vlan2
C   127.0.0.0/8 is directly connected, 30:13:18, lo0
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is 20.1.1.2 to network 0.0.0.0

S   0.0.0.0/0 [1/100] via 20.1.1.1, 00:00:07, vlan2
C   20.1.1.0/24 is directly connected, 00:00:08, vlan2
C   100.1.1.0/24 is directly connected, 00:00:13, vlan3
C   127.0.0.0/8 is directly connected, 29:17:19, lo0
```

Step 4: Check the result. Use the **ping** command to verify the connectivity between PC1 and PC2

#On PC1, use the ping command to check the connectivity.

```
C:\Documents and Settings\Administrator>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Reply from 100.1.1.2: bytes=32 time<1ms TTL=125
Reply from 100.1.1.2: bytes=32 time<1ms TTL=125
Reply from 100.1.1.2: bytes=32 time<1ms TTL=125
Reply from 100.1.1.2: bytes=32 time<1ms TTL=125

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1 and PC2 can communicate with each other.

38.3.2 Configure a Floating Static Route *-B -S -E -A*

Network Requirements

- On Device1, configure two static routes to reach network segment 192.168.1.0/24. One route passes Device2, and the other route passes Device3.
- Device1 first uses the route between Device1 and Device2 to forward packets. If the link is faulty, Device1 switches over to the route between Device1 and Device3 for communication.

Network Topology

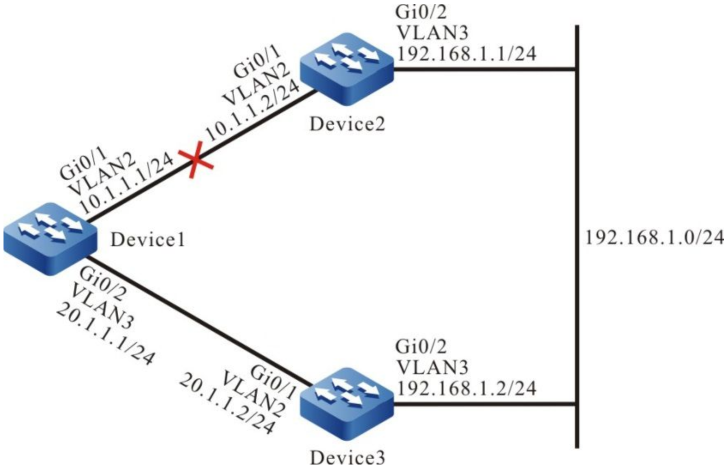


Figure 38-2 Networking for Configure a Floating Static Route

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure static routes.

#On Device1, configure two routes to network segment 192.168.1.0/24 through Device2 and Device3.

```
Device1#configure terminal
Device1(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.2
Device1(config)#ip route 192.168.1.0 255.255.255.0 20.1.1.2
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 02:16:43, vlan2
C   20.1.1.0/24 is directly connected, 03:04:15, vlan3
C   127.0.0.0/8 is directly connected, 14:53:00, lo0
S   192.168.1.0/24 [1/100] via 10.1.1.2, 00:00:05, vlan2
               [1/100] via 20.1.1.2, 00:00:02, vlan3
```

According to the routing tables, two routes from Device1 to network segment 192.168.1.0/24 are reachable, and the route form load balancing.

Step 4: Configure a floating route.

#Configure Device1. Modify the administrative range of the route with the gateway address 20.1.1.2 to 15 so that the route becomes a floating route.

```
Device1(config)#ip route 192.168.1.0 255.255.255.0 20.1.1.2 15
```

Step 5: Check the result.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 02:28:25, vlan2
C   20.1.1.0/24 is directly connected, 03:15:58, vlan3
C   127.0.0.0/8 is directly connected, 15:04:42, lo0
S   192.168.1.0/24 [1/100] via 10.1.1.2, 00:11:47, vlan2
```

According to the routing table, because the route with the administrative range 1 has a higher priority than the route with the administrative range 15, the route with the gateway 20.1.1.2 is deleted.

#After the route between Device1 and Device2 becomes faulty, query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   20.1.1.0/24 is directly connected, 03:23:44, vlan3
C   127.0.0.0/8 is directly connected, 15:12:28, lo0
S   192.168.1.0/24 [15/100] via 20.1.1.2, 00:00:02, vlan3
```

According to the routing table, the route with a larger administrative range has been added to the routing table to forward packets through Device3.

NOTE

- The most significant feature of the floating static route is that it acts as a backup route.

38.3.3 Configure a Static Null0 Interface Route *-S -E -A*

Network Requirements

- Configure a static default route on Device1 and Device2, and the gateway addresses are the peer interface addresses of the two devices. Configure the static Null0 interface route on Device1 to filter only the data to PC2.

Network Topology

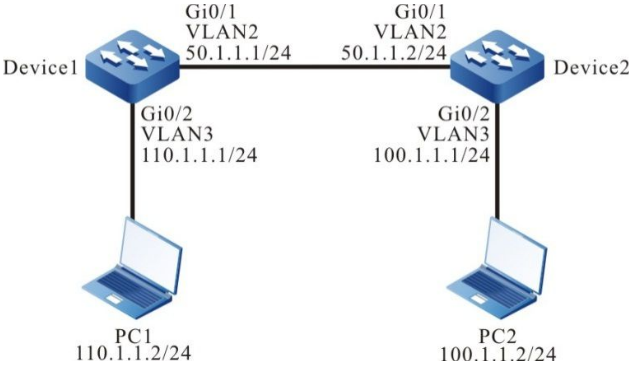


Figure 38-3 Networking for Configuring a Static Null0 Interface Route

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure static route.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ip route 0.0.0.0 0.0.0.0 50.1.1.2
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ip route 0.0.0.0 0.0.0.0 50.1.1.1
```

#On PC1, use the **ping** command to verify connectivity to PC2.

```
C:\Documents and Settings\Administrator>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Reply from 100.1.1.2: bytes=32 time<1ms TTL=126
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 4: Configure a static Null0 interface route.

#Configure Device1.

```
Device1(config)#ip route 100.1.1.2 255.255.255.255 null0
```

Step 5: Check the result.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is 50.1.1.2 to network 0.0.0.0

S   0.0.0.0/0 [1/100] via 50.1.1.2, 00:07:28, vlan2
C   50.1.1.0/24 is directly connected, 00:07:34, vlan2
C   110.1.1.0/24 is directly connected, 00:00:08, vlan3
C   127.0.0.0/8 is directly connected, 11:46:35, lo0
S   100.1.1.2/32 [1/1] is directly connected, 00:02:31, null0
```

The static Null0 interface route has been added to the routing table.

#On PC1, use the ping command to verify connectivity to PC2.

```
C:\Documents and Settings\Administrator>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.1.1.2:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

After the ICMP packet sent by PC1 searches the routing table on Device1, it is found that the output interface is Null0 and is discarded directly, so PC1 cannot communicate with PC2.

NOTE

- The static Null0 interface route is a special route and the datagrams sent to the Null0 interface will be discarded; so a static Null0 interface route can be configured to filter packets.

38.3.4 Configure a Static Recursive Route *-B -S -E -A*

Network Requirements

- On Device1, configure two static routes to reach network segment 192.168.1.1/32. One route passes Device2, and the other passes Device3. Device1 first uses the route that passes Device3 to forward packets.
- On Device1, configure a static recursive route to reach network segment 200.0.0.0/24, with the gateway address being the loopback interface address 192.168.1.1 of Device3. After the route between Device1 and Device3 is faulty, Device1 switches to

the route that passes Device2 for communication.

Network Topology

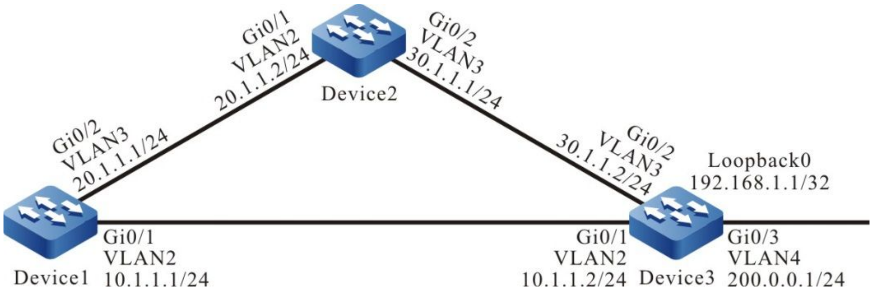


Figure 38-4 Networking for Configure a Static Recursive Static Route

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure static routes.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ip route 192.168.1.1 255.255.255.255 10.1.1.2
Device1(config)#ip route 192.168.1.1 255.255.255.255 20.1.1.2 10
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ip route 192.168.1.1 255.255.255.255 30.1.1.2
```

Step 4: Configure a static recursive route.

#Configure Device1.

```
Device1(config)#ip route 200.0.0.0 255.255.255.0 192.168.1.1
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 00:04:07, vlan2
C   20.1.1.0/24 is directly connected, 00:03:58, vlan3
C   127.0.0.0/8 is directly connected, 73:10:12, lo0
S   200.0.0.0/24 [1/100] via 192.168.1.1, 00:00:08, vlan2
S   192.168.1.1/32 [1/100] via 10.1.1.2, 00:01:46, vlan2
```

According to the routing table, the gateway address of the route to 200.0.0.0/24 is 192.168.1.1, the output interface is VLAN2, and the route relies on the route to 192.168.1.1/32.

Step 5: Check the result.

#After the route between Device1 and Device3 becomes faulty, query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   20.1.1.0/24 is directly connected, 00:09:04, vlan3
C   127.0.0.0/8 is directly connected, 73:15:18, lo0
S   200.0.0.0/24 [1/100] via 192.168.1.1, 00:00:02, vlan3
S   192.168.1.1/32 [10/100] via 20.1.1.2, 00:00:02, vlan3
```

Comparing the routing table information with the routing table information in Step 3, the output interface has changed to VLAN3, indicating that the route has been switched to the route to Device2.

38.3.5 Configure a Static Route to Link with BFD *-E -A*

Network Requirements

- Two static routes are configured on Device1 to the network segment 201.0.0.0/24, one accessible through Device2 and the other accessible through Device3. Device1 has priority in forwarding packets using the line between Device3 and Device1. Similarly, two static routes are configured on Device3 to the network segment 200.0.0.0/24. Device3 has priority in forwarding packets using the line between Device3 and Device1.
- A static route is configured on Device1 and Device3 to link with BFD. After a fault occurs in the line between Device1 and Device3, the static route quickly switches to Device2 for communication.

Network Topology

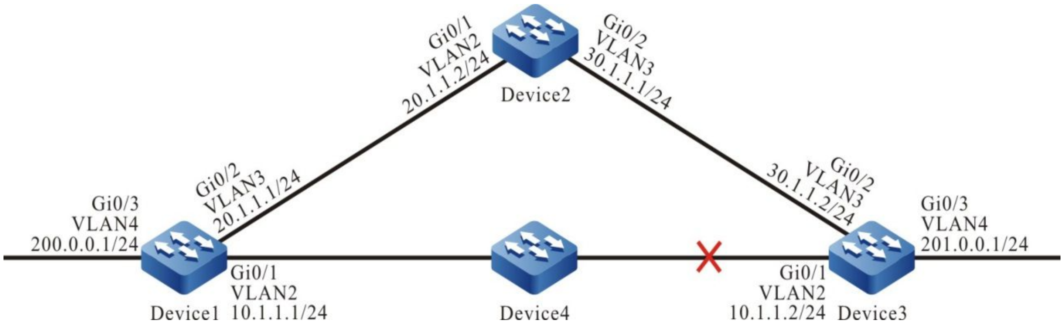


Figure 38-5 Networking for Configuring a Static Route to Link with BFD

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure static route.

#Configure Device1 and configure two static routes to the network segment 201.0.0.0/24.

```
Device1#configure terminal
```

```
Device1(config)#ip route 201.0.0.0 255.255.255.0 vlan2 10.1.1.2
Device1(config)#ip route 201.0.0.0 255.255.255.0 vlan3 20.1.1.2 10
```

#Configure Device2 and configure two static routes to the network segments 200.0.0.0/24 and 201.0.0.0/24, respectively.

```
Device2#configure terminal
Device2(config)#ip route 200.0.0.0 255.255.255.0 20.1.1.1
Device2(config)#ip route 201.0.0.0 255.255.255.0 30.1.1.2
```

#Configure Device3 and configure two static routes to the network segment 200.0.0.0/24.

```
Device3#configure terminal
Device3(config)#ip route 200.0.0.0 255.255.255.0 vlan2 10.1.1.1
Device3(config)#ip route 200.0.0.0 255.255.255.0 vlan3 30.1.1.1 10
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 00:07:41, vlan2
C   20.1.1.0/24 is directly connected, 00:07:29, vlan3
C   127.0.0.0/8 is directly connected, 101:56:14, lo0
C   200.0.0.0/24 is directly connected, 00:15:33, vlan4
S   201.0.0.0/24 [1/100] via 10.1.1.2, 00:02:23, vlan2
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 00:10:21, vlan2
C   30.1.1.0/24 is directly connected, 00:10:09, vlan3
C   127.0.0.0/8 is directly connected, 126:44:08, lo0
S   200.0.0.0/24 [1/100] via 10.1.1.1, 00:06:12, vlan2
C   201.0.0.0/24 is directly connected, 00:20:37, vlan4
```

Step 4: Configure a static route to link with BFD.

#Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#ip route static bfd vlan2 10.1.1.2
```

#Configure Device3.

```
Device3(config)#bfd fast-detect
Device3(config)#ip route static bfd vlan2 10.1.1.1
```

Step 5: Check the result.

#Query the BFD session of Device1.

```
Device1#show bfd session
OurAddr          NeighAddr          LD/RD          State       Holddown      interface
10.1.1.1         10.1.1.2           15/22          UP          5000          vlan2
```

#Query the BFD session of Device3.

```
Device3#show bfd session
OurAddr          NeighAddr          LD/RD          State       Holddown      interface
10.1.1.2         10.1.1.1           22/15          UP          5000          vlan2
```

The normal establishment of a BFD session on Device1 and Device3 indicates that the static route coordinates with BFD successfully.

#When a fault occurs in the line between Device1 and Device3, BFD can quickly detect the line fault and switch to Device2 for communication. Query the BFD session and routing table of Device1.

```
Device1#show bfd session
OurAddr          NeighAddr          LD/RD          State       Holddown      interface
10.1.1.1         10.1.1.2           15/0           DOWN        5000          vlan2

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 00:29:07, vlan2
C   20.1.1.0/24 is directly connected, 00:28:55, vlan3
C   127.0.0.0/8 is directly connected, 102:17:40, lo0
C   200.0.0.0/24 is directly connected, 00:36:58, vlan4
S   201.0.0.0/24 [10/100] via 20.1.1.2, 00:00:09, vlan3
```

The BFD on Device3 is handled similarly to Device1.

39 RIP

39.1 Overview

On the current Internet, it is impossible to run only one gateway protocol. You can divide it into multiple Autonomous Systems (ASs), each of which has its own routing technology. The internal routing protocols within an AS are Interior Gateway Protocols (IGPs). Routing Information Protocol (RIP) is one type of IGP. RIP adopts the Vector-Distance algorithm. RIP features simple and easy-to-use, so it is widely used in numerous small-sized networks.

RIP has two versions: RIPv1 and RIPv2. RIPv1 does not support classless routing, and RIPv2 supports classless routing. Usually, RIPv2 is used.

RIP is a simple protocol which provides simple configuration. However, the number of routes to be advertised by RIP is directly proportional to the number of routes in the routing table. If the number of routes is large, a lot of device resources and network resources are consumed. In addition, RIP specifies that the maximum number of hops that a routing path that passes routers is 15, so RIP is applicable only to simple small- and medium-sized network. RIP is applicable for most campus networks and LANs with a simple structure and strong continuity. For a more complex environment, RIP is not recommended.

RIPv1 was introduced earlier in RFC1058, but it has many deficiencies. To improve the deficiencies of RIPv1, RFC1388 introduced RIPv2, which was then revised in RFC 1723 and RFC 2453.

NOTE

Only the MTS2800 series switch supports this function.

39.2 RIP Function Configuration

Table 39-1 RIP Function List

Configuration Tasks	
Configure basic functions of RIP.	Enables RIP globally.
	Enable RIP for VRF.
	Configure RIP versions.
Configure RIP route generation.	Configure RIP to advertise the default route.

Configuration Tasks	
	Configure RIP to re-distribute routes.
Configure RIP route control.	Configure the administrative distance of RIP.
	Configure an RIP route summary.
	Configure the RIP metric offset.
	Configure RIP route filtration.
	Configure the metric of the RIP interface.
	Configure the routing flag for an RIP interface.
	Configure the maximum load balancing for RIP.
Configure RIP network authentication.	Configure RIP network authentication.
Configure RIP network optimization.	Configure RIP timers.
	Configure RIP split horizon and toxicity reverse of RIP.
	Configure source address check.
	Configure a static RIP neighbor.
	Configure a passive RIP interface.
	Configure RIP to trigger updates.
	Configure an RIP backup interface.

39.2.1 Configure Basic Functions of RIP *-S -E -A*

Configuration Conditions

Before configuring the basic functions of RIP, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- The network layer addresses of the interfaces have been configured so that the adjacent network nodes are reachable at the network layer.

Enable RIP Globally

Before using RIP, make the following configurations:

- Create an RIP process.
- Configure RIP to cover a directly connected network or interface.

Table 39-2 Enabling RIP Globally

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create an RIP process and enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure RIP to cover a specified network segment or interface.	**network** { *ip-address* | *interface-name* }	Mandatory. By default, RIP does not cover any directly connected network or interface.

NOTE

- The covered network segment is categorized into classful addresses.
- You cannot use the **network** *ip-address* command to cover super network addresses. To cover super network addresses, use the **network** *interface-name* command.

Enable RIP for VRF

To enable RIP to support VRF functions, make the following configurations:

- Configure a VRF and add an interface to the VRF.
- Enable the RIP function in the VRF address family.
- Configure RIP to cover a VRF directly connected network or interface.

Table 39-3 Enable RIP for VRF

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Create an RIP process and enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Enter the VRF address family configuration mode of the RIP protocol.	**address-family** { **ipv4 vrf** *vrf-name* }	Mandatory. By default, the VRF address family mode is disabled.
Configure RIP to cover a specified network segment or interface.	**network** { *ip-address* | *interface-name* }	Mandatory. By default, RIP does not cover any directly connected network or interface.

NOTE

- To enable RIP in VRF mode, you must first create VRF-related configurations.

Configure RIP Versions

RIP has two versions, RIPv1 and RIPv2. They can be configured in three modes: global configuration mode, VRF configuration mode, and interface configuration mode.

- By default, RIPv1 is enabled in global configuration mode and VRF configuration mode, and it is not configured in interface configuration mode.
- The version configuration command in interface configuration mode is a higher priority than the version configuration command in global or VRF configuration mode.
- If the version configuration command is not configured, the command in VRF configuration mode of the interface to which the VRF belongs or the command global configuration mode is used.
- In interface configuration mode, the RIP transmit version and the RIP receive version can be configured independently.
- After versions are configured, RIP has strict packet transmitting and receiving processing: In the case of RIPv1, the interface transmits and receives only RIPv1 broadcast and unicast packets. In the case of RIPv2, the interface can transmit and receive RIPv2 unicast, multicast, and broadcast packets. In the case of RIPv1 compatible mode, the interface can transmit RIPv2 unicast and broadcast packets.

Table 39-4 Configuring RIP Versions

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Create an RIP process and enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure the global RIP version.	**version** { 1 | 2 }	Mandatory. By default, RIPv1 is enabled.
Enter the RIP VRF configuration mode.	**address-family** { **ipv4 vrf** *vrf-name* }	Mandatory. By default, the VRF address family mode is disabled.
Configure the RIP version in RIP VRF configuration mode.	**version** { 1 / 2 }	Mandatory. By default, RIPv1 is enabled.
Return to the RIP configuration mode.	**exit-address-family**	-
Return to the global configuration mode.	**exit**	-
Enter the interface configuration mode.	**interface** *interface_name*	-
Configure the RIP transmit version of the interface.	**ip rip send version** {{ 1 / 2 } | 1-compatible }	Optional. By default, the interface transmits packets based on the global RIP version.
Configure the RIP receive version of the interface.	**ip rip receive version** { 1 / 2 }	Optional. By default, the interface receives packets based on the global RIP version.

39.2.2 Configure RIP Route Generation *-S -E -A*

Configuration Conditions

Before configuring RIP route generation, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- RIP is enabled.

Configure RIP to Advertise the Default Route

Through configuration, a device can send the default route on all RIP interfaces to set itself as the default gateway of other neighbor devices.

Table 39-5 Configure RIP to Advertise the Default Route

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure RIP to advertise the default route.	**default-information originate**	Mandatory. By default, RIP does not advertise the default route.

NOTE

- If a default route (0.0.0.0/0) is learnt, the default route (0.0.0.0/0) advertised by the local device is replaced. When a loop exists in a network, network flapping may be caused. In using this command, prevent other devices in the same routing domain from enabling the command at the same time.

Configure RIP to Re-distribute Routes

By redistributing routes, you can introduce the routes generated by other protocols to RIP.

Table 39-6 Configuring RIP to Re-distribute Routes

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.

Step	Command	Description
Configure the default metric for the routes of other protocols introduced to RIP.	**default-metric** *metric-value*	Optional. By default, the default metric of the introduced routes of other protocols is 1.
Configure RIP to Re-distribute routes.	**redistribute** *protocol* [*protocol-id*] [**metric** *metric-value*] [**route-map** *route-map-name*] [**match** *route-sub-type*]	Mandatory. By default, route Re-distribution is not configured.

NOTE

- If the metric command option is specified during Re-distribution, the Re-distributed route adopts the metric.
- In configuring RIP to Re-distribute routes, the available *match* options for the applied route policy include ip address, route type, and tag, and the available set options for the applied route policy include interface, ip next-hop, route source, and metric.

39.2.3 Configure RIP Route Control *-S -E -A*

Configuration Conditions

Before configuring RIP route control, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- RIP is enabled.

Configure the Administrative Distance of RIP

One device can run multiple routing protocols at the same time. The device selects the optimal route from the routes that are learnt from different protocols based on the administrative distances. The smaller the administrative distance is, the higher the priority is.

Table 39-7 Configuring the Administrative Distance of RIP

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-

Step	Command	Description
Enter the RIP configuration mode.	**router rip**	-
Configure the administrative distance of RIP.	**distance** *distance-value*	Mandatory. By default, the administrative distance of RIP is 120.

Configure an RIP Route Summary

Through RIP route summary, a routing device summarizes subnet routes in a natural network segment to form a summary route. The summary route and the original subnet routes all exist in the RIP routing table.

After RIP route summary is configured, the device advertises only the route summary. This greatly decreases the size of adjacent RIP routing tables in a medium- and large-sized network and decreases the consumption of the network bandwidth by routing protocol packets.

A route summary takes the minimum value among metrics of all subnet routes as its metric.

RIPv1 supports automatic route summary mode, and RIPv2 supports the automatic route summary mode and the manual summary mode.

1. RIP auto route summary

Different from manual route summary, auto route summary enables RIP to automatically generate a natural mask route based on subnet routes in one natural network segment.

Table 39-8 Configure the Auto Route Summary Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure the auto route summary function of RIPv2.	**auto-summary**	Mandatory. By default, the auto route summary function of RIPv2 is disabled, but the auto route summary function of RIPv1 is enabled.

NOTE

- RIPv1 does not support the route summary command.
- The tag of a route summary is 0, and minimum metric of the routes is taken as the route summary metric. If the auto route summary is configured, auto route summary has the priority.
- Exercise caution in using the auto route summary function. Ensure that it is necessary to perform auto route summary; otherwise, routing loops may be caused.
- When the auto route summary function of RIPv2 is enabled, if the interface of the advertised route and the route are in the same natural network segment, the update packet sent from the interface does not result in summary of all subnet routes in the natural network segment; otherwise, routes are gathered to form a natural network segment and then it is advertised.

2. Manual route summary

In manual route summary, a combination of a destination address and a mask need to be configured. The combination gathers all routes in the covered network segment for route summary.

Table 39-9 Configuring the Manual Route Summary Function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure the manual route summary function of RIPv2 on the interface.	**ip summary-address rip** *prefix-address*	-

Configure the RIP Metric Offset

By default, RIP applies the route metric advertised by the neighbor device to the received routes. To modify the metric in some special application scenarios, you can configure the RIP metric offset to correct the metric of the specified route.

If the metric in the incoming direction is configured, RIP modifies the metric of the received routes and saves the routes into the routing table. When RIP advertises a metric to the neighbor devices, it advertises the new metric. If the metric in the outgoing direction is configured, the metric is modified only when RIP advertises a metric to the neighbor devices.

Table 39-10 Configuring the RIP Metric Offset

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure RIP to modify the metric of the specified route.	**offset-list** *access-list-name* { **in** | **out** } *metric-offset* [*interface-name*]	Mandatory. By default, no metric is configured for any interface.

NOTE

- Route metric offset supports only matching a standard access list.

Configure RIP Route Filtration

A router can filter the received or advertised routes by configuring an Access Control List (ACL) or prefix list. In receiving RIP routes, you can filter some learnt routes; or in announcing RIP routes, you can filter some routes that are advertised to neighbor devices.

Table 39-11 Configuring RIP Route Filtration

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure the RIP route filtration function.	**distribute-list** { *access-list-name* | **prefix** *prefix-list-name* } { **in** | **out** } [*interface-name*]	Mandatory. By default, the route filtration function is not configured. During the configuration process of the route filtration function, if no interface is specified, route filtration is

Step	Command	Description
		enabled for all routes that are received and transmitted by all the interfaces covered by RIP.

NOTE

- In filtration based on ACL, only a standard ACL is supported.

Configure the Metric of the RIP Interface

If an interface is overwritten by an RIP process, the corresponding direct route is generated in the database, with the default metric 1. When the route is in the RIP database or it is advertised to neighbor devices, if the interface is configured with a metric, the interface metric is used as the metric of the route.

If the interface metric is changed, the RIP database immediately updates the corresponding direct route of RIP and advertises the new metric to the neighbor devices.

Table 39-12 Configuring the Metric of the RIP Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure the metric of the RIP interface.	**ip rip metric** *metric-value*	Mandatory. By default, the RIP interface metric is 1.

NOTE

- Configuring the RIP interface metric affects only the metric of the direct subnet of the interface while it does not affect the metric learned by routes.

Configure the Routing Flag for an RIP Interface

The network administrator can attach tags to some routes. Then, in applying a route policy, the network administrator can perform route filtration or route property advertisement based on the tags.

Only the routing tags of RIPv2 are supported.

Table 39-13 Configuring the Routing Flag for an RIP Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure a tag for the route of the direct subnet of the interface.	**ip rip tag** *tag-value*	-

Configure the Maximum Number of RIP Load Balancing Entries

This command helps you to control the number of RIP load balancing entries for routing.

Table 39-14 Configuring the Maximum Number of RIP Load Balancing Entries

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure the maximum number of RIP load balancing entries.	**maximum-paths** *max-number*	Optional. By default, the maximum number of RIP load balancing entries is 4.

39.2.4 Configure RIP Network Authentication *-S -E -A*

RIPv2 supports protocol packet authentication, therefore, it can satisfy the high security requirement of some networks. Currently, plain text authentication and Message Digest 5 (MD5) authentication are supported. Plain text authentication features low security because it transmits plain text. MD5 converts an authentication code into the MD5 code for transmission, ensuring higher security.

Owing to the limit of RIPv2 packets, a packet that advertises a route contains only 16 bytes. Therefore, the length of a plain text authentication string must not exceed 16 bytes. Meanwhile, the MD5 code that is converted from any character string is a standard 16-byte code, meeting the requirement on the string length.

Table 39-15 Configuring RIP Network Authentication

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure RIPv2 network authentication.	**ip rip authentication** { { **key** { 0 | 7 } *key-string* } | { **key-chain** *key-chain-name* } | { **mode** { **text** | **md5** } } }	Mandatory. By default, the IPv2 authentication function is not configured.

NOTE

- Before implementing MD5 authentication, pay attention to the following points:
- RIPv1 does not support network authentication.
- RIPv2 supports one authentication mode at a time.
- Key ID must be carried in the MD5 authentication information. If you use the **ip rip authentication key** command to configure a password, the key ID is 1. If you use the **ip rip authentication key-chain** command to configure a password, the key ID is the key ID in Key-chain.
- In obtaining a packet transmit authentication password from Key-chain, select a Key ID in the sequence of from small to large. Therefore, the Key ID with the smallest valid transmit password will be selected.
- In obtaining a packet receive authentication password from Key-chain, select the first valid receive password whose Key ID is equal to or larger than the packet receive Key ID. Therefore, if Key IDs are different for the two ends of authentication, the end with the larger Key ID can pass the authentication while the end with the smaller Key ID fails in the authentication.

39.2.5 Configure RIP Network Optimization *-S -E -A*

Configuration Conditions

Before configuring RIP network optimization, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- RIP is enabled.

Configure RIP Timers

RIP does not maintain neighbor relations and it does not support route withdrawn; therefore, the protocol provides four configurable timers to control the network convergence speed. The four timers are: route update timer, router timeout timer, route dampening update timer, and route clear timer.

The route timeout time must be at least three times of the route update time. If no route update packet is received within the route timeout time, the route becomes invalid and it enters a dampening cycle. The length of the dampening cycle is determined by the dampening update time. During the cycle, the route will not be cleared. After the dampening cycle is completed, the route enters the clear cycle. During the cycle, the route can be updated. However, if no route update packet is received during the cycle, the route will be deleted.

Table 39-16 Configuring RIP Timers

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure RIP timers.	**timers basic** *update-interval invalid-interval holddown-interval flush-interval*	Optional. By default, the RIP update interval is 30s, the valid time for advertisement is 180s, the dampening time is 180s, and the clear time is 240s.

NOTE

- In the same RIP routing domain, the **timer basic** configurations on all the devices must be the same to prevent network flapping.

Configure RIP Split Horizon and Toxicity Reverse of RIP

Split horizon and toxicity reverse are mechanisms that are used to prevent route loops.

1. Configure split horizon.

RIP does not advertise routes that it has learnt from an interface to the interface, preventing routing loops.

Table 39-17 Configuring RIP Split Horizon

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configuring RIP split horizon.	**ip split-horizon**	Mandatory. By default, the split horizon function is disabled.

2. Configure toxicity reverse.

RIP announces routes that have been learnt from an interface to the interface, but the route metric is the maximum number of hops, 16, preventing routing loops.

Table 39-18 Configuring RIP Toxicity Reverse

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure RIP toxicity reverse.	**ip split-horizon poisoned**	Optional. By default, the toxicity reverse function is enabled.

NOTE

- The split horizon and toxicity reverse functions are valid only for the learnt routes, direct routes in the network covered by RIP, and the Re-distributed direct and static routes.
- The split horizon function and the toxicity reversion function cannot be used at the same time.

Configure RIP Source Address Check

Through source address check, RIP checks the source addresses of the received packets. RIP processes only the packets whose source addresses meet the requirements. The check items include: the packet source address is in the same network segment as the input interface address; the packet source address matches the peer end address of the Point-to-Point (P2P) interface.

By default, RIP is enabled to check whether the source addresses received through the Ethernet port are in the same network segment as the address of the interface, and this function cannot be cancelled.

Table 39-19 Configuring RIP Source Address Check

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure RIP to start source address check on the P2P interface.	**validate-update-source check-p2p-destination**	Mandatory. By default, the peer address of the P2P interface is not checked.

Configure a Static RIP Neighbor

RIP does not maintain neighbor relations, so it does not have the concept of neighbor. Here the neighbor refers to the neighbor RIP routing device. After a static RIP neighbor is specified, RIP sends RIP packets to the neighbor in unicast mode. The configuration is applied to a network that does not support broadcast or multicast, such as point-to-point links. If the configuration is applied to a broadcast or multicast network, it may cause repeated RIP packets in the network.

Table 39-20 Configuring a Static RIP Neighbor

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure advertisement of routes to a neighbor in unicast mode.	**neighbor** *ip-address*	Mandatory. The parameter ip-address is the IP address of the peer direct-connect interface.

NOTE

- RIP advertises routes only to the interfaces that it covers, and the passive interface setting cannot prevent an interface from sending packets to its static neighbor.

Configure a Passive RIP Interface

To decrease the network bandwidth consumed by the routing protocol, the dynamic routing protocol uses the passive interface function. RIP receives only route update packets on a passive interface, and it does not send route update packets on the passive interface. In a low-speed network with small bandwidth, the passive interface function and the neighbor function cooperate to effectively reduce interactions of RIP routes.

Table 39-21 Configuring a Passive RIP Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the RIP configuration mode.	**router rip**	Mandatory. By default, the RIP process is disabled.
Configure a passive RIP interface.	**passive-interface** { **default** | *interface-name* }	Mandatory. By default, no passive interface is configured.

NOTE

- The passive interface function does not restrain an interface from sending unicast route updates to its neighbor devices. When the passive interface function is used with the **neighbor** command, the function does not restrain an interface from sending unicast route updates to its neighbor devices. This application mode controls a router so that it sends route updates only to some neighbor devices in unicast mode instead of sending route updates to all neighbor devices in broadcast mode (or multicast mode in the case of RIPv2).

Configure RIP to Trigger Updates

After a device receives an RIP update packet, to reduce the possibility of introducing loops owning to routing table differences, the device advertises the update packet of the route to its neighbor devices immediately instead of waiting for the update timer to time out before an update. The update trigger mechanism speeds up network convergence.

Table 39-22 Configuring RIP to Trigger Updates

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure RIP to trigger updates on the interface.	**ip rip triggered**	Optional. By default, the update trigger function is disabled.

Configure an RIP Standby Interface

To speed up backup route convergence, RIP newly supports a backup interface (standby interface) function. On the main route interface of RIP, specify a backup interface for the main interface. In a specific application environment, RIP learns RIP routes only from one line, and the backup line does not provide routing information interaction. If the main interface gets offline, RIP sends Request packets to the peer end through the backup interface periodically (Default: 1s) to request for all routes. If the backup interface receives a Response packet from the peer route, RIP cancels sending of Request packets. It updates the local routing table, and advertises the local routing table to the backup interface. If the backup interface fails to receive a Response packet from the peer end before timeout, RIP cancels sending of Request packets.

Table 39-23 Configuring an RIP Backup Interface

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the interface configuration mode.	**interface** *interface-name*	-
Configure an RIP backup interface.	**ip rip standby** *interface-name* [**timeout** *timeout-value*]	Optional. By default, the backup interface function is disabled, and the default *timeout-value* is 300s.

39.2.6 Configure RIP to Link with BFD *-E -A*

A backup interface can only be applied to a specific application environment and cannot meet the requirements of real-time backup. At this point, RIP provides BFD function for end-to-end protection, which can realize fast convergence and switching of the route. BFD provides a method for quickly detecting the state of the line between two devices. When BFD detection is enabled between two neighbor RIP devices, if there is a line fault between the devices, BFD will quickly detect the fault and notify RIP protocol, and RIP will delete the RIP route associated with the BFD interface. If a backup route exists for these routes, these routes will be switched to the backup route in a very short time (affected by the BFD configuration). Currently, RIP only supports BFD single-hop bidirectional detection.

Table 39-24 Configure RIP to Link with BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIP configuration mode	**router rip**	Required By default, the RIP process is disabled.
Configure all interfaces covered by RIP process to enable BFD function	**bfd all-interfaces**	Required By default, the BFD function of all interfaces covered by RIP is disabled
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the BFD function enabled on the interface	**ip rip bfd**	Required By default, the interface BFD function is disabled

NOTE

- Refer to the reliability technology - BFD technical manual for relevant BFD configuration.

39.2.7 RIP Monitoring and Maintaining *-S -E -A*

Table 39-25 RIP Monitoring and Maintaining

Command	Description
show ip rip [**vrf** *vrf-name*]	Display the basic information about the RIP protocol.
show ip rip [**vrf** *vrf-name*] **database** [**detail** | *prefix/mask* [[**detail** | **longer-prefixes** [**detail**]]]]	Display the information about the RIP routing database.
show ip rip [**vrf** *vrf-name*] **statistics**	Display the RIP protocol statistics.
show ip rip interface [*interface-name*]	Display the RIP interface information.
clear ip rip [**vrf** *vrf-name*] { **process** | **statistics** }	Clears RIP process and statistics.

39.3 RIP Typical Configuration Example

39.3.1 Configure the RIP Version *-S -E -A*

Network Requirements

- RIPv2 runs between Device1 and Device2 for route interaction.

Network Topology

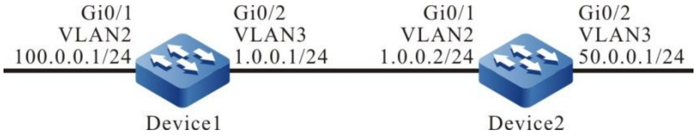


Figure 39-1 Networking for Configuring the RIP Version

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
```

```
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 100.0.0.0
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 50.0.0.0
Device2(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan3
R   50.0.0.0/8 [120/1] via 1.0.0.2, 00:13:26, vlan3
C   100.0.0.0/24 is directly connected, 00:23:06, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan2
C   50.0.0.0/24 is directly connected, 00:23:06, vlan3
R   100.0.0.0/8 [120/1] via 1.0.0.1, 00:13:26, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

According to the routing table, the route advertised by the device uses an 8-bit natural mask.

Step 4: Configure the RIP version.

#Configure Device1.

```
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#exit
```

Step 5: Check the result.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan3
```

```
R   50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C   100.0.0.0/24 is directly connected, 00:23:06, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan2
C   50.0.0/24 is directly connected, 00:23:06, vlan3
R   100.0.0.0/24 [120/1] via 1.0.0.1, 00:13:26, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

According to the routing table, the route advertised by the device uses a 24-bit accurate mask.

39.3.2 Configure RIP to Re-distribute Routes *-S -E -A*

Network Requirements

- OSPF runs between Device1 and Device2. Device2 learns OSPF routes 100.0.0.0/24 and 200.0.0.0/24 advertised by Device1.
- RIPv2 runs between Device2 and Device3. Device2 Re-distributes OSPF route 100.0.0.0/24 to RIP and advertises the route to Device3.

Network Topology

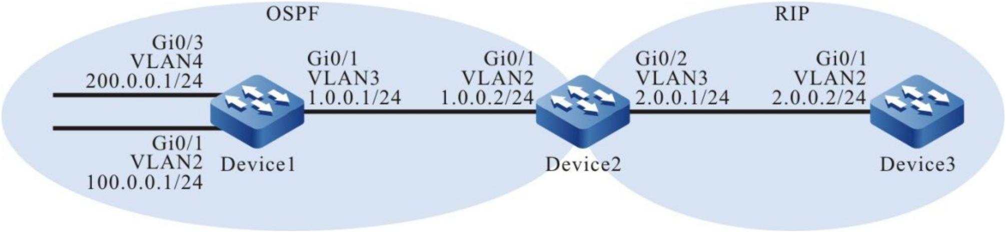


Figure 39-2 Networking for Configuring RIP to Re-distribute Routes

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure OSPF.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
```

```
Device2(config-ospf)#exit
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   100.0.0.0/24 [110/2] via 1.0.0.1, 00:04:12, vlan2
O   200.0.0.0/24 [110/2] via 1.0.0.1, 00:04:12, vlan2
```

According to the routing table, Device2 has learnt the OSPF routes that have been advertised by Device1.

Step 4: Configure RIP.

#Configure Device2.

```
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#exit
```

Step 5: Configure the route policy.

#On Device2, configure route-map to invoke ACL to match 100.0.0.0/24 and filter 200.0.0.0/24.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map OSPFtoRIP
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#exit
```

NOTE

- In configuring a route policy, you can create a filtration rule based on a prefix list or ACL. The prefix list can precisely match routing masks while the ACL cannot match routing masks.

Step 6: Configure RIP to Re-distribute routes.

#Configure Device2.

```
Device2(config)#router rip
Device2(config-rip)#redistribute ospf 100 route-map OSPFtoRIP
Device2(config-rip)#exit
```

Step 7: Check the result.

#Query the RIP routing table of Device2.

```
Device2#show ip rip database
Types: N - Network, L - Learn, R - Redistribute, D - Default config, S - Static config
Proto: C - connected, S - static, R - RIP, O - OSPF, E - IRMP,
       o - SNSP, B - BGP, i-ISIS

RIP routing database in VRF kernel (Counter 3):
T/P Network          ProID Metric Next-Hop       From          Time  Tag   Interface
N/C 2.0.0.0/24        none  1       --             --            --   0    vlan3
R/O 100.0.0.0/24       1     1      1.0.0.1         --            --   0    vlan2
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 00:23:06, vlan2
R   100.0.0.0/24 [120/1] via 2.0.0.1, 00:13:26, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

By querying the RIP routing table on Device2 and the querying the routing table on Device3, it is found that route 100.0.0.0/24 on Device2 has been Re-distributed to RIP and route 200.0.0.0/24 has been successfully filtered out.

NOTE

- In an actual application, if there are two or more AS boundary routers, it is recommended that you do not Re-distribute routes between different routing protocols. If route Re-distribution must be configured, you are required to configure route control policies such as route filtration and filtration summary on the AS boundary routers to prevent routing loops.

39.3.3 Configure the RIP Metric Offset *-S -E -A*

Network Requirements

- RIPv2 runs between Device1, Device2, Device3, and Device4.
- Device1 learns route 200.0.0.0/24 from both Device2 and Device3.
- On Device1, set the route metric offset in the receive direction so that Device1 selects the route advertised by Device2 with priority.

Network Topology

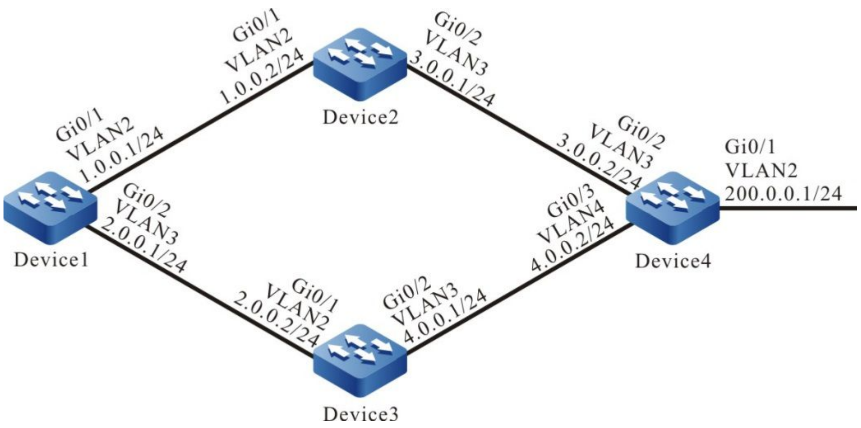


Figure 39-3 Networking for Configuring the RIP Metric Offset

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 4.0.0.0
Device3(config-rip)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router rip
Device4(config-rip)#version 2
Device4(config-rip)#network 3.0.0.0
Device4(config-rip)#network 4.0.0.0
Device4(config-rip)#network 200.0.0.0
Device4(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan2
C   2.0.0.0/24 is directly connected, 00:22:56, vlan3
R   3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R   4.0.0.0/24 [120/1] via 2.0.0.2, 00:11:04, vlan3
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
R   200.0.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
             [120/2] via 2.0.0.2, 00:08:31, vlan3
```

According to the routing table of Device1, two routes to 200.0.0.0/24 are available.

Step 4: Configure the ACL.

#Configure Device1.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
```

Step 5: Configure a metric offset.

#On Device1, configure the metric offset list and increase the metric of the route that has been learnt from interface VLAN3 and matches AL to 3.

```
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

Step 6: Check the result.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:33:59, vlan2
C   2.0.0.0/24 is directly connected, 00:33:50, vlan3
R   3.0.0.0/24 [120/1] via 1.0.0.2, 00:24:20, vlan2
R   4.0.0.0/24 [120/1] via 2.0.0.2, 00:21:57, vlan3
C   127.0.0.0/8 is directly connected, 77:01:54, lo0
R   200.0.0.0/24 [120/2] via 1.0.0.2, 00:19:25, vlan2
```

According to the routing table of Device1, the next-hop output interface of route 200.0.0.0/24 is only VLAN2, indicating that Device1 has selected the route advertised by Device2 with priority.

NOTE

- The route metric offset list can be applied to all interfaces or a specified interface, and it can be used in both the receiving and advertisement directions.

39.3.4 Configure RIP Route Filtration *-S -E -A*

Network Requirements

- RIPv2 runs between Device1 and Device2 for route interaction.
- Device1 learns two routes 2.0.0.0/24 and 3.0.0.0/24 that have been advertised by Device2, and then it filters route 3.0.0.0/24 in the advertisement direction of Device2.

Network Topology

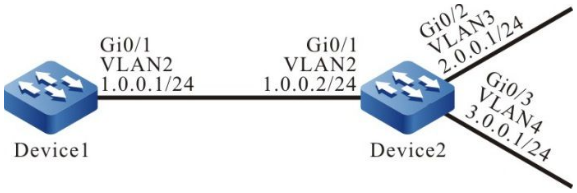


Figure 39-4 Networking for Configuring RIP Route Filtration

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan2
R   2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R   3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

According to the routing table, Device1 has learnt two routes advertised by Device2.

Step 4: Configure the ACL.

#Configure Device2.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 2.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
```

NOTE

- In configuring route filtration, you can create a filtration rule based on a prefix list or ACL. The prefix list can precisely match routing masks while the ACL cannot match routing masks.

Step 5: Configure route filtration.

#Configure route filtration in the output direction of interface VLAN2 of Device2.

```
Device2(config)#router rip
Device2(config-rip)#distribute-list 1 out vlan2
Device2(config-rip)#exit
```

Step 6: Check the result.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan2
R   2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

According to the routing table, Device2 does not advertise route 3.0.0.0/24 to Device1, but the route is deleted from the routing table of Device only after the route times out.

NOTE

- The **distribute-list** can be applied to all interfaces or a specified interface, and it can be used in both the receiving and advertisement directions.

39.3.5 Configure an RIP Route Summary *-S -E -A*

Network Requirements

- RIPv2 runs between Device1, Device2, Device3, and Device4 for route interaction.
- Device1 learns two routes 100.1.0.0/24 and 100.2.0.0/24 from Device2. To reduce the size of the routing table of Device1, it is required that Device advertises only the route summary of the two routes to Device1.

Network Topology

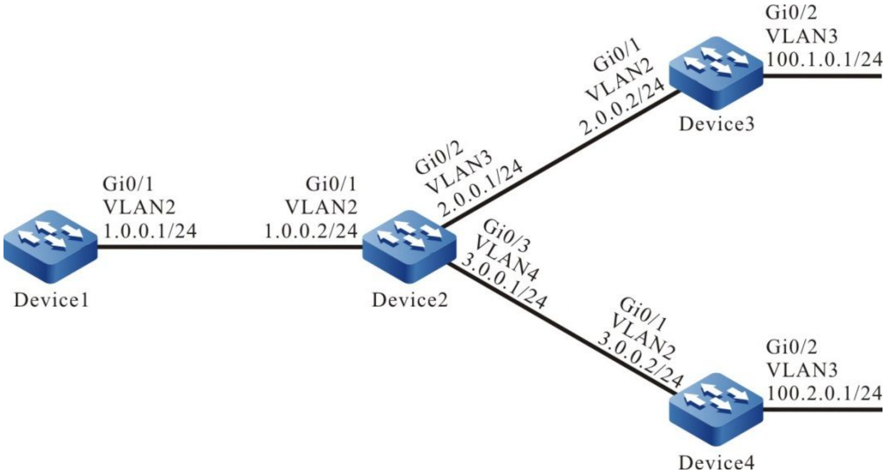


Figure 39-5 Networking for Configuring RIP Route Summary

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
```

```
Device3(config-rip)#network 100.0.0.0
Device3(config-rip)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router rip
Device4(config-rip)#version 2
Device4(config-rip)#network 3.0.0.0
Device4(config-rip)#network 100.0.0.0
Device4(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan2
R   2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R   3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R   100.1.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
R   100.2.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

Step 4: Configure a summary of routes on an interface.

#On Device2, configure a route summary 100.0.0.0/8.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip summary-address rip 100.0.0.0/8
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:24:06, vlan2
R   2.0.0.0/24 [120/1] via 1.0.0.2, 00:14:26, vlan2
R   3.0.0.0/24 [120/1] via 1.0.0.2, 00:14:26, vlan2
R   100.0.0.0/8 [120/2] via 1.0.0.2, 00:00:31, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

On Device1, the route summary 100.0.0.0/8 advertised by Device2 and learnt by Device1 is displayed. The two routes that are contained in the route summary can be deleted only after timeout.

NOTE

- RIP supports global auto route summary and interface manual route summary. In RIPv2, the global auto route summary function is disabled.

39.3.6 Configure RIP to Link with BFD *-E -A*

Network Requirements

- Run RIPv2 between Device1, Device2 and Device3 for route interaction.
- Device1 learns route 3.0.0.0/24 from both Device2 and Device3. Configure the route offset so that Device1 selects the route advertised by Device2 with priority. Between Device1 and Device2 is the main line of the route; between Device1 and Device3 is the backup line of the route.
- Configure BFD between Device1 and Device2. When a fault occurs on the line between Device1 and Device2, it is necessary to configure an RIP between Device1 and Device2 to link with BFD, so as to quickly detect the line fault. When BFD detects the main line fault, it will trigger RIP to update the route, and the route 3.0.0.0/24 is switched to the backup line.

Network Topology

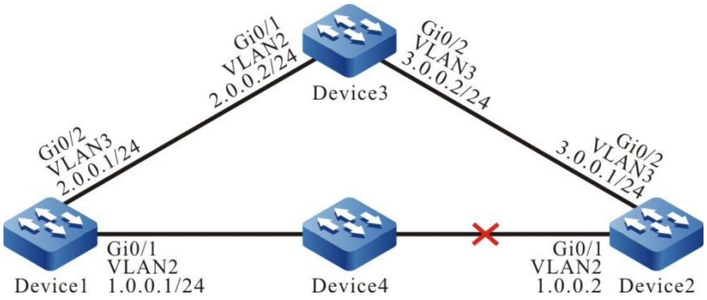


Figure 39-6 Networking for Configuring RIP to Link with BFD

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure RIP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
```

```
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 3.0.0.0
Device3(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 01:30:23, vlan2
C   2.0.0.0/24 is directly connected, 01:30:14, vlan3
R   3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
         [120/1] via 2.0.0.2, 00:00:02, vlan3
C   127.0.0.0/8 is directly connected, 77:58:18, lo0
```

Device1 learns route 3.0.0.0/24 from both Device2 and Device3.

Step 4: Configure a route offset.

#Configure a route offset in the incoming direction of the interface VLAN3 of Device1, so that the metric of the route that matches ACL is increased by 3.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config)#exit
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

```
C   1.0.0.0/24 is directly connected, 01:30:23, vlan2
C   2.0.0.0/24 is directly connected, 01:30:14, vlan3
R   3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
C   127.0.0.0/8 is directly connected, 77:58:18, lo0
```

It can be seen that after the route offset is configured, Device1 selects the route 3.0.0.0/24 advertised by Device2 with priority.

Step 5: Configure BFD.

#Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip rip bfd
Device1(config-if-vlan2)#exit
```

#Configure Device2.

```
Device2(config)#bfd fast-detect
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip rip bfd
Device2(config-if-vlan2)#exit
```

Step 6: Check the result.

#Query BFD information on Device1.

```
Device1#show bfd session
OurAddr          NeighAddr        LD/RD        State      Holddown     interface
1.0.0.1          1.0.0.2          2/4          UP         5000         vlan2
```

#After a fault occurs on the line between Device1 and Device2, the route can quickly switch to the backup line.

#Query the route information on Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 02:07:47, vlan3
R   3.0.0.0/24 [120/4] via 2.0.0.2, 00:01:14, vlan3
C   127.0.0.0/8 is directly connected, 78:35:51, lo0
```

39.3.7 Configure an RIP Backup Interface *-S -E -A*

Network Requirements

- RIPv2 runs between Device1, Device2, and Device3 for route interaction.
- Device1 learns route 3.0.0.0/24 from Device2 and Device3. Then, configure route metric offset so that Device1 selects the route advertised by Device2 with priority. At this time, the line between Device1 and Device2 becomes the main line of the route. The line between Device1 and Device3 becomes and backup line of the route.
- On Device1, configure an RIP backup interface. If the main line is normal, the route passes the main line. If the main line is faulty, the route quickly switches to the backup line.

Network Topology

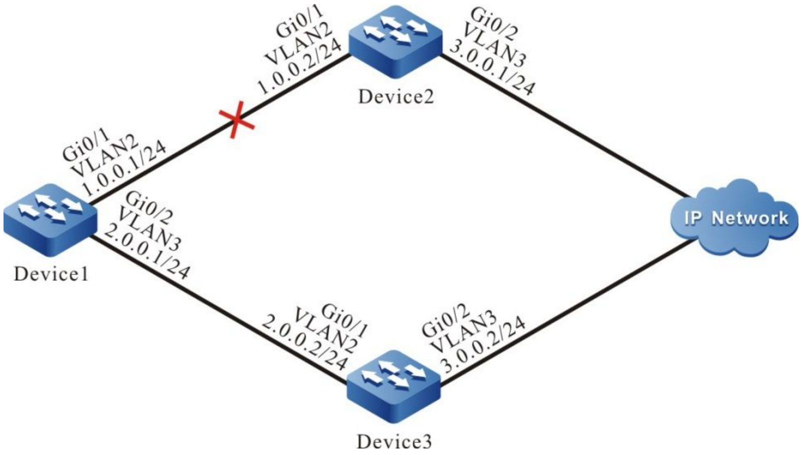


Figure 39-7 Networking for Configuring an RIP Backup Interface

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 3.0.0.0
Device3(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 01:30:23, vlan2
C   2.0.0.0/24 is directly connected, 01:30:14, vlan3
R   3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
             [120/1] via 2.0.0.2, 00:00:02, vlan3
C   127.0.0.0/8 is directly connected, 77:58:18, lo0
```

Device1 has learnt route 3.0.0.0/24 from both Device2 and Device3.

Step 4: Configure a route metric offset.

#On Device1, configure a route metric offset in the input direction of interface VLAN3 so that the metric of the routes that match ACL is increased to 3.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config)#exit
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 01:30:23, vlan2
C   2.0.0.0/24 is directly connected, 01:30:14, vlan3
R   3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
C   127.0.0.0/8 is directly connected, 77:58:18, lo0
```

After the route metric offset is configured, Device1 selects route 3.0.0.0/24 advertised by Device2.

Step 5: Configure a backup interface.

#On Device1, configure interface VLAN3 as the RIP backup interface of VLAN2.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip rip standby vlan3
Device1(config-if-vlan2)#exit
```

Step 6: Check the result.

#If the line between Device1 and Device2 becomes faulty, the route can quickly switch over to the backup line between Device1 and Device3.

#On Device1, query the route information.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 02:07:47, vlan3
R   3.0.0.0/24 [120/4] via 2.0.0.2, 00:01:14, vlan3
C   127.0.0.0/8 is directly connected, 78:35:51, lo0
```

39.3.8 Configure a Passive RIP Interface *-S -E -A*

Network Requirements

- RIPv2 runs between Device1 and Device2 for route interaction.
- On Device1, configure a passive interface which does not send update packets to Device2.

Network Topology

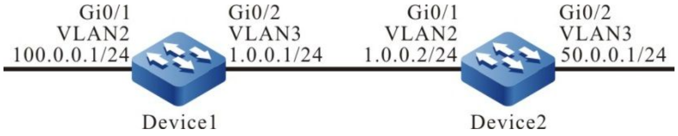


Figure 39-8 Networking for Configuring an RIP Passive Interface

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. (Omitted)

Step 2: Configure IP addresses for the ports. (Omitted)

Step 3: Configure RIP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 100.0.0.0
Device1(config-rip)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 50.0.0.0
Device2(config-rip)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

```
C   1.0.0.0/24 is directly connected, 00:23:06, vlan3
R   50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C   100.0.0.0/24 is directly connected, 00:23:06, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan2
C   50.0.0/24 is directly connected, 00:23:06, vlan3
R   100.0.0.0/24 [120/1] via 1.0.0.1, 00:13:26, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

Step 4: Configure a passive interface.

#Configure Device1.

```
Device1(config)#router rip
Device1(config-rip)#passive-interface vlan3
Device1(config-rip)#exit
```

VLAN3 of Device1 is configured as a passive interface which does not send update packets to Device2, but Device2 can still receive update packets.

Step 5: Check the result.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:23:06, vlan3
R   50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C   100.0.0.0/24 is directly connected, 00:23:06, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
```

Route 50.0.0.0/24 is still kept on Device1. On Device2, after the RIP route times out and is deleted, route 100.0.0.0/24 is deleted from the routing table.

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:25:06, vlan2
C   50.0.0/24 is directly connected, 00:25:06, vlan3
C   127.0.0.0/8 is directly connected, 77:51:00, lo0
```

40 RIPng

40.1 Overview

RIPng, also called RIP next generation, is a dynamic routing protocol for IPv6 network to provide route information for IPv6 packet forwarding. RIPng is extended on RIP-2, and the RIPng protocol works in much the same way as RIP. To accommodate IPv6 networks, RIPng makes the following changes to the existing RIP protocol:

- UDP port number: The RIPng protocol uses the port number 521 of UDP to send and receive protocol packets;
- Multicast address: The RIPng protocol uses FF02::9 as the multicast address of the RIPng router in the local range of the link and does not support broadcast;
- Prefix length: The RIPng protocol route destination address uses a 128-bit prefix length;
- Next-hop address: The RIPng protocol uses a 128-bit IPv6 address;
- Source address: The RIPng protocol uses the local address FE80::/10 of the link as the source address to send RIPng protocol packets.

The protocols related to RIPng include RFC2080 and RFC2081.

40.2 RIPng Function Configuration

Table 40-1 RIPng Function List

Configuration task	
Configure basic functions of RIPng	Enable RIPng globally
Configure RIPng route generation	Configure RIPng to advertise the default route
	Configure RIPng to re-distribute routes
Configure RIPng route control	Configure the administrative distance of RIPng
	Configure an RIPng route summary
	Configure the RIPng metric offset
	Configure RIPng route filtration

Configuration task	
	Configure the metric of the RIPng interface
	Configure the routing flag for an RIPng interface
	Configure the maximum load balancing for RIPng
Configure RIPng network optimization	Configure RIPng timers
	Configure RIPng split horizon and toxicity reverse
	Configure a static RIPng neighbor
	Configure a passive RIPng interface

40.2.1 Configure Basic Functions of RIPng -E -A

Configuration Conditions

Before configuring the basic functions of RIPng, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer;
- The IPv6 capability has been configured to enable the interface.

Enable RIPng Globally

Before using RIPng, make the following configurations:

- Create an RIPng process;
- Configure an interface to enable the RIPng protocol.

Table 40-2 Enabling RIPng Globally

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create an RIPng process and enter the RIPng configuration mode	**ipv6 router rip** *process-id*	Required By default, the RIPng process is disabled.
Exit the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-

Steps	Command	Description
The interface enables the RIPng protocol	**ipv6 rip enable** *process-id*	Required By default, the interface disables the RIPng protocol

40.2.2 Configure RIPng Route Generation -E -A

Configuration Conditions

Before configuring RIPng route generation, ensure that:

- The IPv6 capability has been configured to enable the interface;
- RIPng is enabled.

Configure RIPng to Advertise the Default Route

Through configuration, a device can send the default route on all RIPng interfaces to set itself as the default gateway of other neighbor devices.

Table 40-3 Configure RIPng to Advertise the Default Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIPng configuration mode	**ipv6 router rip** *process-id*	Required By default, the RIPng process is disabled.
Configure RIPng to advertise the default route	**default-information originate** [**metric** *value*]	Required By default, RIPng does not advertise the default route

NOTE

- If a default route (::/0) is learnt, the default route (::/0) advertised by the local device is replaced. When a loop exists in a network, network flapping may be caused. In using this command, prevent other devices in the same routing domain from enabling the command at the same time.

Configure RIPng to Re-distribute Routes

By redistributing routes, you can introduce the routes generated by other protocols to RIPng.

Table 40-4 Configure RIPng to Re-distribute Routes

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIPng configuration mode	**ipv6 router rip** *process-id*	Required By default, the RIPng process is disabled.
Configure the default metric for the routes of other protocols introduced to RIPng	**default-metric** *metric-value*	Optional By default, the default metric of the introduced routes of other protocols is 1
Configure RIPng to re-distribute routes	**redistribute** *protocol* [*protocol-id*] [**metric** *metric-value*] [**route-map** *route-map-name*] [**match** *route-sub-type*]	Required By default, route Re-distribution is not configured.

NOTE

- If the metric command option is specified during Re-distribution, the Re-distributed route adopts the metric.
- In configuring RIPng to Re-distribute routes, the available match options for the applied route policy include ipv6 address, route type, tag, interface, ipv6 nexthop, ipv6 route-source and metric, and the available set options include metric and tag.

40.2.3 Configure RIPng Route Control *-E -A*

Configuration Conditions

Before configuring RIPng route control, ensure that:

- The IPv6 capability has been configured to enable the interface;
- RIPng is enabled.

Configure the Administrative Distance of RIPng

One device can run multiple routing protocols at the same time. The device selects the optimal route from the routes that are learnt from different protocols based on the administrative distances. The smaller the administrative distance is, the higher the priority is.

Table 40-5 Configuring the Administrative Distance of RIPng

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIPng configuration mode	**ipv6 router rip** *process-id*	-
Configure the administrative distance of RIPng	**distance** *distance-value*	Required By default, the administrative distance of RIPng is 120

Configure an RIPng Route Summary

Through RIPng route summary, a combination of a pair of destination addresses and masks is configured to summarize the routes within the covered network segment.

After RIPng route summary is configured, the device advertises only the route summary. This greatly decreases the size of adjacent RIPng routing tables in a medium- and large-sized network and decreases the consumption of the network bandwidth by routing protocol packets.

A route summary takes the minimum value among metrics of all subnet routes as its metric.

Table 40-6 Configure the RIPng Route Summary Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the route summary function of RIPng on the interface	**ipv6 rip summary-address** *prefix-address*	Required By default, the route summary function is not configured.

Configure the RIPng Metric Offset

By default, RIPng applies the route metric advertised by the neighbor device to the received routes. To modify the metric in some special application scenarios, you can configure the RIPng metric offset to correct the metric of the specified route.

If the metric in the incoming direction is configured, RIPng modifies the metric of the received routes and saves the routes into the routing table. When RIPng advertises a metric to the neighbor devices, it advertises the new metric. If the metric in the outgoing direction is configured, the metric is modified only when RIPng advertises a metric to the neighbor devices.

Table 40-7 Configuring the RIPng Metric Offset

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIPng configuration mode	**ipv6 router rip** *process-id*	Required By default, the RIPng process is disabled.
Configure RIPng to modify the metric of the specified route	**offset-list** *access-list-name* { **in** | **out** } *metric-offset* [*interface-name*]	Required By default, no metric is configured for any interface.

Configure RIPng Route Filtration

A router can filter the received or advertised routes by configuring an Access Control List (ACL), prefix list or routing map. In receiving RIPng routes, you can filter some learnt routes; or in announcing RIPng routes, you can filter some routes that are advertised to neighbor devices.

Table 40-8 Configuring RIPng Route Filtration

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIPng configuration mode	**ipv6 router rip** *process-id*	Required By default, the RIPng process is disabled.
Configure the RIPng route filtration function	**distribute-list** { *access-list-name* | **prefix** *prefix-list-name* | **route-map** *route-map-name*} { **in | out** } [*interface-name*]	Required By default, the route filtration function is not configured. During the configuration process of the route filtration function, if no interface is specified, route filtration is enabled for all RIPng interfaces

Configure the metric of the RIPng interface

After an interface enables RIPng, the corresponding direct route is generated in the database, with the default metric 1. When the route is in the RIPng database or it is advertised to neighbor devices, if the interface is configured with a metric, the interface metric is used as the metric of the route.

If the interface metric is changed, the RIPng database immediately updates the corresponding direct route of RIPng and advertises the new metric to the neighbor devices.

Table 40-9 Configuring the Metric of the RIPng Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the metric of the RIPng interface	**ipv6 rip metric** *metric-value*	Required By default, the metric of the RIPng interface is 1

NOTE

- Configuring RIPng interface metric affects only the metric of the direct subnet of the interface while it does not affect the metric learned by routes.

Configure the routing flag for an RIPng interface

The network administrator can attach tags to some routes. Then, in applying a route policy, the network administrator can perform route filtration or route property advertisement based on the tags.

Table 40-10 Configuring the Routing Flag for an RIPng Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure a tag for the route of the direct subnet of the interface.	**ipv6 rip tag** *tag-value*	Required By default, the route tag is not configured

Configure the Maximum Number of RIPng Load Balancing Entries

This command helps you to control the number of RIPng load balancing entries for routing.

Table 40-11 Configuring the Maximum Number of RIPng Load Balancing Entries

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIPng configuration mode	**ipv6 router rip** *process-id*	Required By default, the RIPng process is disabled.
Configure the Maximum Number of RIPng Load Balancing Entries	**maximum-paths** *max-number*	Optional By default, the Maximum Number of RIPng Load Balancing Entries is 4

40.2.4 Configure RIPng Network Optimization *-E -A*

Configuration Conditions

Before configuring RIPng network optimization, ensure that:

- The IPv6 capability has been configured to enable the interface;
- RIPng is enabled.

Configure RIPng Timers

RIPng does not maintain neighbor relations and it does not support route withdrawn; therefore, the protocol provides four configurable timers to control the network convergence speed. The four timers are: route update timer, router timeout timer, route dampening update timer, and route clear timer.

The route timeout time must be at least three times of the route update time. If no route update packet is received within the route timeout time, the route becomes invalid and it enters a dampening cycle. The length of the dampening cycle is determined by the dampening update time. During the cycle, the route will not be cleared. After the dampening cycle is completed, the route enters the clear cycle. During the cycle, the route can be updated. However, if no route update packet is received during the cycle, the route will be deleted.

Table 40-12 Configuring RIPng Timers

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIPng configuration mode	**ipv6 router rip** *process-id*	Required By default, the RIPng process is disabled.

Steps	Command	Description
Configure RIPng timers	**timers** *update-interval invalid-interval holddown-interval flush-interval*	Optional By default, the RIPng update interval is 30s, the valid time for advertisement is 180s, the dampening time is 0s, and the clear time is 240s.

NOTE

- In the same RIPng routing domain, the timer basic configurations on all the devices must be the same to prevent network flapping.

Configure RIPng Split Horizon and Toxicity Reverse

Split horizon and toxicity reverse are mechanisms that are used to prevent route loops.

1. Configure split horizon.

RIPng does not advertise routes that it has learnt from an interface to the interface, preventing routing loops.

Table 40-13 Configuring RIPng Split Horizon

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configuring RIPng split horizon.	**no ipv6 split-horizon** [**disable**]	Optional By default, the split horizon function is enabled

2. Configure toxicity reverse

RIPng announces routes that have been learnt from an interface to the interface, but the route metric is the maximum number of hops, 16, preventing routing loops.

Table 40-14 Configuring RIPng Toxicity Reverse

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure RIPng toxicity reverse	**ipv6 split-horizon poison-reverse**	Required By default, the toxicity reverse function is disabled

NOTE

- The split horizon and toxicity reverse functions are valid only for the learnt routes, direct routes of RIPng interface, the Re-distributed direct and static routes.
- The split horizon function and the toxicity reversion function cannot be used at the same time.

Configure a static RIPng Neighbor

RIPng does not maintain neighbor relations, so it does not have the concept of neighbor. Here the neighbor refers to the neighbor RIPng routing device. After a static RIPng neighbor is specified, RIPng sends RIPng packets to the neighbor in unicast mode. The configuration is applied to a network that does not support broadcast or multicast, such as point-to-point links. If the configuration is applied to multicast network, it may cause repeated RIP packets in the network.

Table 40-15 Configuring a Static RIPng Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure advertisement of routes to a neighbor in unicast mode	**ipv6 rip neighbor** *ipv6-address*	Required The parameter ipv6-address is the ipv6 address of the peer direct-connect interface

NOTE

- RIPng advertises routes only to the interfaces that it covers, and "**ipv6 rip passive**" cannot prevent an interface from sending packets to its static neighbor.

Configure a passive RIPng interface

To decrease the network bandwidth consumed by the routing protocol, the dynamic routing protocol uses the passive interface function. RIPng receives only route update packets on a passive interface, and it does not send route update packets on the passive interface. In a low-speed network with small bandwidth, the passive interface function and the neighbor function cooperate to effectively reduce interactions of RIPng routes.

Table 40-16 Configuring a Passive RIPng Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure a passive RIPng interface	**ipv6 rip passive**	Required By default, no passive interface is configured.

NOTE

- The **ipv6 rip passive** does not restrain an interface from sending unicast route updates to its neighbor devices. When the passive interface function is used with the neighbor command, **ipv6 rip passive** does not restrain an interface from sending unicast route updates to its neighbor devices. This application mode controls a router so that it sends route updates only to some neighbor devices in unicast mode instead of sending route updates to all neighbor devices in broadcast mode.

40.2.5 Configure RIPng to Link with BFD *-E -A*

A backup interface can only be applied to a specific application environment and cannot meet the requirements of real-time backup. At this point, RIPng provides BFD (Bidirectional Forwarding Detection) function for end-to-end protection, which can realize fast convergence and switching of the route. BFD provides a method for quickly detecting the state of the line between two devices. When BFD detection is enabled between two neighbor RIPng devices, if there is a line fault between the devices, BFD will quickly detect the fault and notify RIPng protocol, and RIP will delete the RIPng route associated with the BFD interface. If a backup route exists for these routes, these routes will be switched to the backup route in a very short time (affected by the BFD configuration). Currently, RIPng only supports BFD single-hop bidirectional detection.

Table 40-17 Configure RIPng to Link with BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the RIPng configuration mode	**ipv6 router rip 100**	Required By default, the RIPng process is disabled.
Configure all interfaces covered by RIPng process to enable BFD function	**bfd all-interfaces**	Required By default, the BFD function of all interfaces covered by RIPng is disabled
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the BFD function enabled on the interface	**ipv6 rip bfd**	Required By default, the interface BFD function is disabled

NOTE

- Refer to the reliability technology - BFD technical manual for relevant BFD configuration.

40.2.6 RIPng Monitoring and Maintaining *-E -A*

Table 40-18 Configuring RIPng Monitoring and Maintaining

Command	Description
clear ipv6 rip [*process-id*]{ **process** | **statistics** }	Clear RIPng process and statistics

Command	Description
show ipv6 rip [*process-id*]	Display the basic information about the RIPng protocol
show ipv6 rip [*process-id*] **database** [**detail** | *ipv6-address/mask-length* [**detail** | **longer-prefixes**]]	Display the information about the RIPng routing database
show ipv6 rip [*process-id*] **statistics** [*interface-name*]	Display the RIPng protocol statistics
show ipv6 rip interface [*interface-name*]	Display the RIPng interface information

40.3 RIPng Typical Configuration Example

40.3.1 Configure Basic Functions of RIPng *-E -A*

Network Requirements

- RIPng runs between Device1 and Device2 for route interaction.

Network Topology

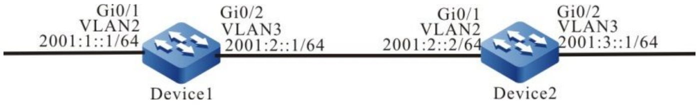


Figure 40-1 Networking for Configuring the Basic Functions of RIPng

Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (omitted)

Step 2: Configure IPv6 addresses for the ports. (omitted)

Step 3: Configure RIPng.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
```

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

Step 4:   Check the result.

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
   via ::, 2w4d:19:31:05, lo0
C   2001:1::/64 [0/0]
   via ::, 00:21:42, vlan2
L   2001:1::1/128 [0/0]
   via ::, 12:21:40 AM, lo0
C   2001:2::/64 [0/0]
   via ::, 12:21:34 AM, vlan3
L   2001:2::1/128 [0/0]
   via ::, 12:21:33 AM, lo0
R   2001:3::/64 [120/2]
   via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

#Query the IPv6 routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
```

```
     via ::, 3d:10:39:31 PM, lo0
R   2001:1::/64 [120/2]
     via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C   2001:2::/64 [0/0]
     via ::, 12:30:46 AM, vlan2
L   2001:2::2/128 [0/0]
     via ::, 12:30:45 AM, lo0
C   2001:3::/64 [0/0]
     via ::, 12:29:12 AM, vlan3
L   2001:3::1/128 [0/0]
     via ::, 12:29:11 AM, lo0
```

According to the routing table, the route advertised by the device uses a 64-bit accurate mask.

40.3.2 Configure RIPng to Re-distribute Routes *-E -A*

Network Requirements

- IPv6 OSPF runs between Device1 and Device2. Device2 learns IPv6 OSPF routes 2001:1::/64 and 2001:2::/64 advertised by Device1.
- RIPng runs between Device2 and Device3. Device2 Re-distributes IPv6 OSPF route 2001:1::/64 to RIPng and advertises the route to Device3.

Network Topology

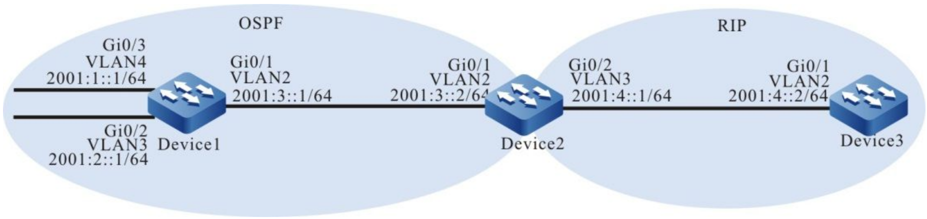


Figure 40-2 Networking for Configuring RIPng to Re-distribute Routes

Configuration Steps

Step 1: Configure VLANs, and add ports to the required VLANs. (omitted)

Step 2: Configure IPv6 addresses for the ports. (omitted)

Step 3: Configure IPv6 OSPF.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)# router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
```

```
Device1(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan4)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan2)#exit
```

#Query the IPv6 routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 4d:12:09:49 AM, lo0
O   2001:1::/64 [110/2]
    via fe80::201:7aff:fe01:204, 12:12:16 AM, vlan2
O   2001:2::/64 [110/2]
    via fe80::201:7aff:fe01:204, 12:12:16 AM, vlan2
C   2001:3::/64 [0/0]
    via ::, 12:19:51 AM, vlan2
L   2001:3::2/128 [0/0]
    via ::, 12:19:50 AM, lo0
C   2001:4::/64 [0/0]
    via ::, 12:45:13 AM, vlan3
L   2001:4::1/128 [0/0]
    via ::, 12:45:12 AM, lo0
```

According to the routing table, Device2 has learnt the IPv6 OSPF routes that have been advertised by Device1.

Step 4: Configure RIPng.

#Configure Device2.

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
Device3(config-if-vlan2)#exit
```

Step 5: Configure the route policy.

#On Device2, configure route-map to invoke prefix list to match 2001:1::/64 and filter 2001:2::/64.

```
Device2(config)#ipv6 prefix-list OSPF permit 2001:1::/64
Device2(config)#route-map OSPFtoRIP
Device2(config-route-map)#match ipv6 address prefix-list OSPF
Device2(config-route-map)#exit
```

NOTE

- In configuring a route policy, you can create a filtration rule based on a prefix list or ACL. The prefix list can precisely match routing masks while the ACL cannot match routing masks.

Step 6: Configure RIPng to re-distribute IPv6 OSPF route.

#Configure RIPng to re-distribute IPv6 OSPF route.

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#redistribute ospf 100 route-map OSPFtoRIP
Device2(config-ripng)#exit
```

Step 7: Check the result.

#Query the RIPng database of Device2.

```
Device2#show ipv6 rip database
```

```
Type : N - Network interface, L - Learn, R - Redistribute, D - Default config,
    S - Static config
Proto: C - connected, S - static, R - RIP, O - OSPF, E - IRMP,
    o - SNSP, B - BGP, i-ISIS

RIPng process 100 routing database (VRF Kernel, Counter 2):
[Type/Proto]
[R/O] 2001:1::/64 metric 1
       via vlan2, fe80::201:7aff:fe01:204, no expires
[N/C] 2001:4::/64 metric 1, installed
       via vlan3, ::, no expires
```

#Query the IPv6 routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
   via ::, 2w0d:8:00:11 PM, lo0
R   2001:1::/64 [120/2]
   via fe80::201:7aff:fec3:38a5, 2:50:14 AM, vlan2
C   2001:4::/64 [0/0]
   via ::, 3:56:24 AM, vlan2
L   2001:4::2/128 [0/0]
   via ::, 3:56:23 AM, lo0
```

By querying the database on Device2 and the routing table on Device3, it is found that route 2001:1::/64 on Device2 has been Re-distributed to RIPng and successfully advertised to Device3 and route 2001:2::/64 has been successfully filtered out.

NOTE

- In an actual application, if there are two or more AS boundary routers, it is recommended that you do not Re-distribute routes between different routing protocols. If route Re-distribution must be configured, you are required to configure route control policies such as route filtration and filtration summary on the AS boundary routers to prevent routing loops.

40.3.3 Configure the RIPng Metric Offset *-E -A*

Network Requirements

- RIPng runs between Device1, Device2, Device3, and Device4
- Device1 learns route 2001:5::/64 from both Device2 and Device3.

- On Device1, set the route metric offset in the receive direction so that Device1 selects the route advertised by Device2 with priority.

Network Topology

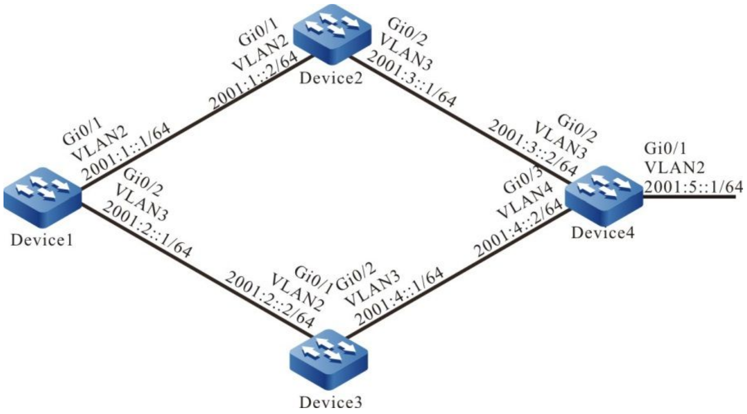


Figure 40-3 Networking for Configuring the RIPng Metric Offset

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 addresses for the ports. (omitted)

Step 3: Configure RIPng.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 rip enable 100
Device3(config-if-vlan3)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#ipv6 router rip 100
Device4(config-ripng)#exit
Device4(config)#interface vlan 2
Device4(config-if-vlan2)#ipv6 rip enable 100
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan 3
Device4(config-if-vlan3)#ipv6 rip enable 100
Device4(config-if-vlan3)#exit
Device4(config)#interface vlan 4
Device4(config-if-vlan4)#ipv6 rip enable 100
Device4(config-if-vlan4)#exit
```

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
    via ::, 2w5d:6:21:24 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:02:05 AM, vlan2
L   2001:1::1/128 [0/0]
    via ::, 12:02:04 AM, lo0
C   2001:2::/64 [0/0]
    via ::, 12:02:02 AM, vlan3
L   2001:2::1/128 [0/0]
    via ::, 12:02:01 AM, lo0
R   2001:3::/64 [120/2]
```

```
    via fe80::201:7aff:fec3:38a4, 12:02:03 AM, vlan2
R   2001:4::/64 [120/2]
    via fe80::201:7aff:fe11:2214, 12:00:48 AM, vlan3
R   2001:5::/64 [120/3]
    via fe80::201:7aff:fec3:38a4, 12:02:03 AM, vlan2
            [120/3]
    via fe80::201:7aff:fe11:2214, 12:00:48 AM, vlan3
```

According to the routing table of Device1, two routes to 2001:5::/64 are available.

Step 4: Configure the ACL.

```
Device1(config)#ipv6 access-list extended RIPng
Device1(config-v6-list)#permit 10 2001:5::/64 any
Device1(config-v6-list)#exit
```

Step 5: Configure a metric offset.

#On Device1, configure the metric offset list and increase the metric of the route that has been learnt from interface vlan3 and matches ACL to 3.

```
Device1(config)# ipv6 router rip 100
Device1(config-ripng)#offset-list RIPng in 3 vlan 3
Device1(config-ripng)#exit
```

Step 6: Check the result.

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 2w5d:6:34:28 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:15:09 AM, vlan2
L   2001:1::1/128 [0/0]
    via ::, 12:15:08 AM, lo0
C   2001:2::/64 [0/0]
    via ::, 12:15:06 AM, vlan3
L   2001:2::1/128 [0/0]
    via ::, 12:15:05 AM, lo0
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:03:10 AM, vlan2
```

```
R   2001:4::/64 [120/2]
    via fe80::201:7aff:fe11:2214, 12:03:10 AM, vlan3
R   2001:5::/64 [120/3]
    via fe80::201:7aff:fec3:38a4, 12:03:10 AM, vlan2
```

According to the routing table of Device1, the next-hop output interface of route 2001:5::/64 is only vlan2, indicating that Device1 has selected the route advertised by Device2 with priority.

NOTE

- The route metric offset list can be applied to all interfaces or a specified interface, and it can be used in both the receiving and advertisement directions.

40.3.4 Configure RIPng Route Filtration *-E -A*

Network Requirements

- RIPng runs between Device1 and Device2 for route interaction.
- Device1 learns two routes 2001:2::/64 and 2001:3::/64 that have been advertised by Device2, and then it filters route 2001:3::/64 in the advertisement direction of Device2.

Network Topology

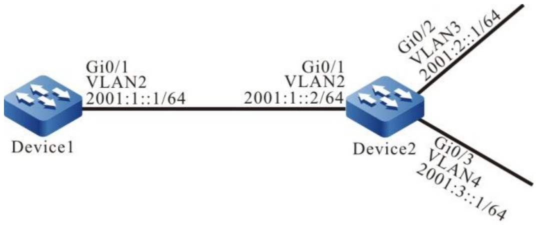


Figure 40-4 Networking for Configuring RIPng Route Filtration

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 addresses for the ports. (omitted)

Step 3: Configure RIPng.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 rip enable 100
Device2(config-if-vlan4)#exit
```

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 2w5d:2:47:44 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:56:34 AM, vlan2
L   2001:1::1/128 [0/0]
    via ::, 12:56:32 AM, lo0
R   2001:2::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:27:11 AM, vlan2
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:27:11 AM, vlan2
```

According to the routing table, Device1 has learnt two routes advertised by Device2.

Step 4: Configure IPv6 prefix list.

```
Device2(config)#ipv6 prefix-list RIPng deny 2001:3::/64
```

Step 5: Configure route filtration.

#Configure route filtration in the output direction of interface VLAN2 of Device2.

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#distribute-list prefix RIPng out vlan 2
Device2(config-ripng)#exit
```

Step 6: Check the result.

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 2w5d:3:03:49 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 1:12:39 AM, vlan2
L   2001:1::1/128 [0/0]
    via ::, 1:12:38 AM, lo0
R   2001:2::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:43:16 AM, vlan2
```

According to the routing table, Device2 does not advertise route 2001:3::/64 to Device1, but the route is deleted from the routing table of Device1 only after the route times out.

NOTE

- The distribute-list can be applied to all interfaces or a specified interface, and it can be used in both the receiving and advertisement directions.

40.3.5 Configure an RIPng Route Summary -E -A

Network Requirements

- RIPng runs between Device1, Device2, Device3, and Device4 for route interaction.
- Device1 learns two routes 2001:4:1:1::/64 and 2001:4:1:2::/64 from Device2. To reduce the size of the routing table of Device1, it is required that Device2 advertises only the route summary of the two routes to Device1.

Network Topology

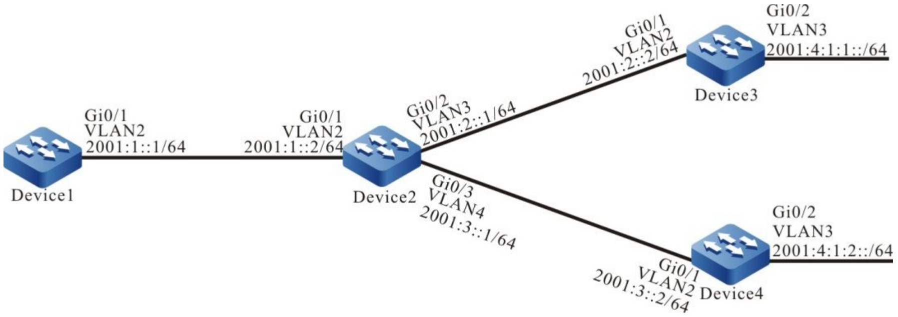


Figure 40-5 Networking for Configuring RIPng Route Summary

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 addresses for the ports. (omitted)

Step 3: Configure RIPng.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ipv6 rip enable 100
Device2(config-if-vlan4)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 rip enable 100
Device3(config-if-vlan3)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#ipv6 router rip 100
```

```
Device4(config-ripng)#exit
Device4(config)#interface vlan 2
Device4(config-if-vlan2)#ipv6 rip enable 100
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan 3
Device4(config-if-vlan3)#ipv6 rip enable 100
Device4(config-if-vlan3)#exit
```

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 2w5d:2:27:40 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:36:29 AM, vlan2
L   2001:1::1/128 [0/0]
    via ::, 12:36:28 AM, lo0
R   2001:2::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:07:06 AM, vlan2
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:07:06 AM, vlan2
R   2001:4:1:1::/64 [120/3]
    via fe80::201:7aff:fec3:38a4, 12:07:06 AM, vlan2
R   2001:4:1:2::/64 [120/3]
    via fe80::201:7aff:fec3:38a4, 12:06:55 AM, vlan2
```

Step 4: Configure a summary of routes on an interface.

#On Device2, configure a route summary 2001:4:1::/48.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip summary-address 2001:4:1::/48
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
    via ::, 2w5d:2:35:44 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:44:33 AM, vlan2
L   2001:1::1/128 [0/0]
    via ::, 12:44:32 AM, lo0
R   2001:2::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:15:10 AM, vlan2
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:15:10 AM, vlan2
R   2001:4:1::/48 [120/3]
    via fe80::201:7aff:fec3:38a4, 12:05:19 AM, vlan2
```

On Device1, the route summary 2001:4:1::/48 advertised by Device2 and learnt by Device1 is displayed. The two routes that are contained in the route summary can be deleted only after timeout.

40.3.6 Configure a Passive RIPng Interface *-E -A*

Network Requirements

- RIPng runs between Device1 and Device2 for route interaction.
- On Device1, configure a passive interface which does not send update packets to Device2.

Network Topology

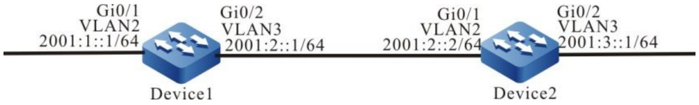


Figure 40-6 Networking for Configuring an RIPng Passive Interface

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 addresses for the ports. (omitted)

Step 3: Configure RIPng.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
```

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 2w4d:19:31:05, lo0
C   2001:1::/64 [0/0]
    via ::, 00:21:42, vlan2
L   2001:1::1/128 [0/0]
    via ::, 12:21:40 AM, lo0
C   2001:2::/64 [0/0]
    via ::, 12:21:34 AM, vlan3
L   2001:2::1/128 [0/0]
    via ::, 12:21:33 AM, lo0
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

#Query the IPv6 routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 3d:10:39:31 PM, lo0
R   2001:1::/64 [120/2]
```

```
    via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C   2001:2::/64 [0/0]
    via ::, 12:30:46 AM, vlan2
L   2001:2::2/128 [0/0]
    via ::, 12:30:45 AM, lo0
C   2001:3::/64 [0/0]
    via ::, 12:29:12 AM, vlan3
L   2001:3::1/128 [0/0]
    via ::, 12:29:11 AM, lo0
```

Step 4: Configure a passive interface.

#Configure Device1.

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip passive
Device1(config-if-vlan3)#exit
```

VLAN3 of Device1 is configured as a passive interface which does not send update packets to Device2, but Device2 can still receive update packets.

Step 5: Check the result.

#Query the IPv6 routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 2w4d:7:55:37 PM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:46:14 AM, vlan2
L   2001:1::1/128 [0/0]
    via ::, 12:46:12 AM, lo0
C   2001:2::/64 [0/0]
    via ::, 12:46:06 AM, vlan3
L   2001:2::1/128 [0/0]
    via ::, 12:46:05 AM, lo0
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 12:35:51 AM, vlan3
```

Route 2001:3::/64 is still kept on Device1. On Device2, after the RIPng route times out and is deleted, route 2001:1::/64 is deleted from the routing table.

#Query the IPv6 routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 3d:11:05:24 PM, lo0
C   2001:2::/64 [0/0]
    via ::, 12:56:39 AM, vlan2
L   2001:2::2/128 [0/0]
    via ::, 12:56:38 AM, lo0
C   2001:3::/64 [0/0]
    via ::, 12:55:05 AM, vlan3
L   2001:3::1/128 [0/0]
    via ::, 12:55:04 AM, lo0
```

41 OSPF

41.1 Overview

OSPF (Open Shortest Path First) is a dynamic routing protocol based on the link status. It uses SPF (Shortest Path First) of Dijkstra to compute the route in a single AS (Autonomous System).

OSPF protocol, developed by IETF, is mainly used to solve the problem of slow convergence and easy loop formation in distance vector routing and is suitable for medium- and large-sized network. The current OSPF2 follows RFC2328 and supports other OSPF extensions as defined by the RFC.

In the OSPF protocol, each device maintains a link state database that describes the AS network, and the devices in the same area have the same database. After the database is fully synchronized, each device takes itself as its root and uses the SPF algorithm to calculate a loop-less SPF tree to describe the shortest path it knows to reach each destination. Finally, each device builds its own routing table from the SPF tree.

The main features of OSPF are

- Fast convergence: immediately send the updated packet after the network topology change and synchronize this change in AS;
- No self-loop: OSPF runs SPF to compute the route according to the link state database, which guarantees that a routing loop will not be formed from the algorithm itself.
- Area division: OSPF allows AS to be divided into multiple areas, so as to reduce the occupation of the network bandwidth and make it possible to build hierarchical networks;
- Support authentication: each time the OSPF device receives a routing protocol packet, it verifies the authentication information in the packet to prevent information leakage or hostile attacks in the network;
- Support subnets of different lengths: the route advertised by OSPF carries a network mask to support subnets of different lengths;
- Support load balance: support multiple ECMPs to the same destination address.

41.2 OSPF Function Configuration

Table 41-1 OSPF Function List

Configuration task	
Configure basic functions of OSPF	Enable OSPF protocol

Configuration task	
Configure OSPF area	Configure OSPF NSSA area
	Configure OSPF Stub area
	Configure an OSPF virtual link
Configure OSPF network type	Configure OSPF interface network type to broadcast
	Configure OSPF interface network type to P2P
	Configure OSPF interface network type to NBMA
	Configure OSPF interface network type to P2MP
Configure OSPF network authentication	Configure OSPF area authentication
	Configure OSPF interface authentication
Configure OSPF route generation	Configure OSPF route Re-distribution
	Configure OSPF default route
	Configure OSPF host route
Configure OSPF route control	Configure OSPF inter-area route summary
	Configure OSPF external route summary
	Configure OSPF inter-area route filtration
	Configure OSPF external route filtration
	Configure OSPF route installation filtration
	Configure the cost value of OSPF interface
	Configure OSPF reference bandwidth
	Configure the administrative distance of OSPF
	Configure the maximum number of OSPF load balancing entries
	Configure the compatible RFC1583 of OSPF

Configuration task	
Configure OSPF network optimization	Configure OSPF neighbor Keepalive time
	Configure a passive OSPF interface
	Configure OSPF demand circuit
	Configure OSPF interface priority
	Configure OSPF interface MTU
	Configure OSPF interface LSA transmit delay
	Configure OSPF LSA retransmit
	Configure OSPF to disable LSA diffusion
	Configure OSPF SPF computation time
	Configure OSPF database overflow
Configure OSPF to link with BFD	Configure OSPF to link with BFD
Configure OSPF GR	Configure OSPF GR Restarter
	Configure OSPF GR Helper

41.2.1 Configure Basic Functions of OSPF *-S -E -A*

In all OSPF configuration tasks, the OSPF protocol must be enabled before the configuration of other features can take effect.

Configuration Conditions

Before configuring the basic functions of OSPF, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer;
- The IP address of the interface is configured to make the adjacent node network layers accessible.

Enable OSPF Protocol

To enable OSPF, you shall first create an OSPF process, specifying the network address range associated with the process and the area to which the address range belongs; if an interface IP address is in the network segment of an area, then the interface belongs to that area and enables OSPF. OSPF advertises the direct route for that interface.

A device running the OSPF protocol must have a Router ID that uniquely identifies a device within an OSPF AS. It is necessary to ensure the uniqueness of the Router ID in the AS, otherwise it will affect the neighbor establishment and route learning. You may specify the Router ID when creating an OSPF process. If the Router ID is not specified, it is selected according to the following rules:

- Select the largest IP address of the Loopback interface as the Router ID;
- If the Loopback interface of IP address is not configured, select the largest IP address from other interfaces as the Router ID;
- Only when the interface is in the UP state can the interface address be selected as the Router ID.

OSPF supports multiple processes and uses the process number to identify a process. Different processes are independent of each other.

Table 41-2 Enable OSPF Protocol

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create an OSPF process and enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	Required Enable OSPF process or enable OSPF process from a VRF. By default, OSPF protocol is disabled by the system. When OSPF is enabled from the VRF, OSPF process belonging to a VRF can only manage the interface belonging to that VRF
Configure the network segment covered by the OSPF area	**network** *ip-address wildcard-mask* **area** *area-id*	Required By default, an interface does not belong to any OSPF process or area An interface can only belong to one OSPF process and area
Configure the Router ID of OSPF process	**router-id** *ip-address*	Optional By default, it is generated according to the election

Steps	Command	Description
		regulation of the Router ID Modifying Router ID will not cause the OSPF neighbor to fail, and the process needs to be manually reset for the newly configured Router ID to take effect

41.2.2 Configure OSPF Area -S -E -A

To reduce the CPU and memory footprint of large amounts of database information, the OSPF AS is divided into a number of areas. The areas are identified by a 32-bit area ID, which can be expressed as a decimal number in the range of 0 to 4294967295 or as an IP address in the range of 0.0.0.0 to 255.255.255.255. Area 0 or 0.0.0.0 represents OSPF backbone area, and other non-0 areas are non-backbone areas. All the inter-area route information needs to be forwarded through the backbone area, and the non-backbone areas cannot exchange the route information directly.

Several types of routers are defined in OSPF:

- Internal Router: a device whose interfaces belong to an area;
- Area Border Router (ABR): a device connected to multiple areas;
- Automonous System Boundary Router (ASBR): a device that introduces external routes to OSPF AS.

Configuration Conditions

Before configuring the OSPF area, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible;
- Enable OSPF protocol.

Configure OSPF NSSA Area

Type-7 LSA instead of Type-5 LSA is allowed to be injected into Not-So-Stub-Area (NSSA). By configuring the Re-distribution, an external route is introduced to the NSSA and the ASBR of NSSA generates a Type-7 LSA and floods into that NSSA. The ABR of NSSA will convert Type-7 LSA to Type-5 LSAs and flood such Type-5 LSAs to the whole AS.

The OSPF NSSA configured through the command **area** *area-id* **nssa no-summary** is called complete NSSA. OSPF complete NSSA disables flooding of inter-area routes. At this point, ABR will generate a default route flooding into the NSSA. Devices in the NSSA will access the network outside the area through this default route.

Table 41-3 Configure OSPF NSSA Area

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure NSSA area	**area** *area-id* **nssa** [[**default-information-originate** [**metric** *metric-value* / **metric-type** *type-value*] / **no-redistribution** / **no-summary** / **translator-role** { **always** | **candidate** | **never** }] | [**translate-always** | **translate-candidate** | **translate-never**]]	Required By default, the area is not an NSSA area

NOTE

- The backbone area cannot be configured as an NSSA area.
- All devices in the same NSSA area must be configured as NSSA area, and devices with inconsistent area types cannot form adjacency relationships.

Configure OSPF Stub Area

A Stub area does not allow AS external routes to flood to reduce the size of the link state database. When an area is configured as a Stub, ABR at the boundary of the Stub generates a default route and floods into the Stub area. Devices in the Stub area will access the network outside AS through this default route.

The OSPF Stub area configured through the command **area** *area-id* **stub no-summary** is called complete Stub. OSPF complete Stub area disables flooding of the inter-area routes and external routes. Devices in the area will access the networks outside the area and OSPF AS through the default route.

Table 41-4 Configure OSPF Stub Area

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-

Steps	Command	Description
Configure Stub area	**area** *area-id* **stub** [**no-summary**]	Required By default, the area is not a Stub area
Configure the cost value of the default route generated by Stub ABR	**area** *area-id* **default-cost** *cost-value*	Optional By default, the cost value of the default route generated by Stub ABR is 1

NOTE

- The backbone area cannot be configured as a Stub area.
- All devices in the same Stub area must be configured as Stub area, and devices with inconsistent area types cannot form adjacency relationships.

Configure an OSPF Virtual Link

The non-backbone areas in OSPF must synchronize databases and interact data through the backbone area. Therefore, it is required that all the non-backbone areas should be connected with the backbone area.

When this requirement is not met in some cases, a virtual link may be configured. After configuring the virtual link, you can configure the authentication method for the virtual link, modify the Hello interval, and so on. These parameters have the same meaning as the general OSPF interface parameters.

Table 41-5Configure an OSPF Virtual Link

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure an OSPF virtual link	**area** *transit-area-id* **virtual-link** *neighbor-id* [[**authentication** [**message-digest** | **null**] | **authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*] / **dead-interval** *seconds* **hello-interval**	Required By default, a virtual link will not be created

Steps	Command	Description
	seconds / **retransmit-interval** *seconds* / **transmit-delay** *seconds*]	

NOTE

- A virtual link must be configured between two ABRs.
- Two ABRs that configure the virtual link must in the same common area, also known as the Transit Area of virtual link.
- The Transit Area of virtual link cannot be Stub or NSSA.

41.2.3 Configure OSPF Network Type *-S -E -A*

OSPF divides the network into four types according to the type of link protocol:

- Broadcast Networks - When the link protocol is Ethernet or FDDI, OSPF default network is broadcast;
- P2P (Point To Point Network) - When the link protocol is PPP, LAPB or HDLC, OSPF default network is P2P;
- NBMA Network - When the link protocol is ATM, frame relay or X.25, OSPF default network is NBMA;
- P2MP (Point To Multi-Point Network) - no link protocol is considered by OSPF to be of type P2MP by default, and non-fully interconnected NBMA is typically configured as OSPF P2MP.

The network type of the OSPF interface can be modified as needed. The interface network type of OSPF neighbors needs to be consistent, otherwise it will affect the normal learning of the route.

Configuration Conditions

Before configuring the OSPF network type, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible;
- Enable OSPF protocol.

Configure OSPF Interface Network Type to Broadcast

Broadcast Networks supports multiple (two or more) devices that have the ability to interact with all devices on the network. OSPF uses Hello packets to dynamically discover neighbors.

Table 41-6 Configure OSPF Interface Network Type to Broadcast

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF interface network type to broadcast	**ip ospf network broadcast**	Required By default, OSPF interface network type is determined by the link layer protocol.

Configure OSPF Interface Network Type to P2P

P2P is a network of two devices, each at one end of the point-to-point link. OSPF uses Hello packets to dynamically discover neighbors.

Table 41-7 Configure OSPF Network Type to P2P

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF network type to P2P	**ip ospf network point-to-point**	Required By default, OSPF interface network type is determined by the link layer protocol.

Configure OSPF Interface Network Type to NBMA

NBMA supports multiple (two or more) devices, but does not have the broadcast capability. The neighbors shall be specified manually.

Table 41-8 Configure OSPF Interface Network Type to NBMA

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF network type to NBMA	**ip ospf network non-broadcast**	Required By default, OSPF interface network type is determined by the link layer protocol.
Enter global configuration mode	**exit**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure an NBMA neighbor	**neighbor** *neighbor-ip-address* [**cost** *cost-value* / **priority** *priority-value* / **poll-interval** *interval-value*]	Required In an NBMA, neighbors are manually specified

Configure OSPF Interface Network Type to P2MP

When NBMA is not fully connected, the network type can be configured as P2MP to save network overhead. In a P2MP, neighbors are manually specified.

Table 41-9 Configure OSPF Interface Network Type to P2MP

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF network type to P2MP	**ip ospf network point-to-multipoint** [**non-broadcast**]	Required By default, OSPF interface network type is determined by the link layer protocol.
Enter global configuration mode	**exit**	-

Steps	Command	Description
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure a P2MP neighbor	**neighbor** *neighbor-ip-address* [**cost** *cost-value* / **priority** *priority-value* / **poll-interval** *interval-value*]	Mandatory if the interface network type is configured as P2MP

41.2.4 Configure OSPF Network Authentication *-S -E -A*

To prevent information leakage or hostile attacks on OSPF devices, all packet interactions between OSPF neighbors have authentication capability. Authentication types can be: NULL (non-authentication), simple text authentication, MD5 and SM3 authentication and key-chain authentication.

After configuring the authentication, the OSPF interface needs to be authenticated before receiving the OSPF protocol packet. Only after passing the authentication, can the OSPF interface receive the packet. Therefore, the authentication method, Key ID and authentication key must be consistent with the OSPF interface for establishing an adjacency relation.

The authentication method and the authentication key are configured independently. When the authentication key is configured, if no authentication method is configured, the authentication method corresponding to the authentication key will be automatically configured.

OSPF authentication can be configured on the area, interface or interface address, with the priority of area authentication, interface authentication and interface address authentication from low to high. That is, the interface address authentication is used first, then the interface authentication and finally the area authentication.

Configuration Conditions

Before configuring OSPF authentication, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible;
- Enable OSPF protocol.

Configure OSPF Area Authentication

OSPF area authentication is only to configure the authentication method and can take effect fully only when the corresponding authentication key is configured under the interface.

Table 41-10 Configure OSPF Area Authentication

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure the area authentication method	**area** *area-id* **authentication** [**message-digest** | **key-chain]**	Required By default, no area authentication is configured In this command, the keyword **message-digest** represents MD5 authentication and **key-chain** represents key-chain authentication, otherwise it is simple text authentication
Enter the interface configuration mode	**interface** *interface-name*	-
Configure a simple text authentication key	**ip ospf** [*ip-address*] **authentication-key** { **0 | 7** } *password*	Required By default, no simple text authentication key is configured
Configure an MD5/SM3 authentication key	**ip ospf** [*ip-address*] **message-digest-key** *key-id {* **md5 | sm3}** { **0** | **7** } *password*	Required By default, no MD5/SM3 authentication key is configured
Configure key-chain authentication	**ip ospf** [*ip-address*] **key-chain** *key-chain name*	Required By default, the **key-chain** authentication is not configured

Configure OSPF Interface Authentication

When there are multiple IP addresses on an OSPF interface, you can specify an authentication method or authentication key for a single interface address. When no interface address is specified, all addresses under the interface adopt the configured authentication method or authentication key.

Table 41-11 Configure OSPF Interface Authentication

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface authentication method	**ip ospf** [*ip-address*] **authentication** [**key-chain | message-digest | null**]	Required By default, no interface authentication method is configured In this command, the keyword **message-digest** represents MD5 authentication, **key-chain** represents key-chain authentication and **null** represents non-authentication, otherwise it is simple text authentication
Configure a simple text authentication key	**ip ospf** [*ip-address*] **authentication-key** { **0 | 7** } *password*	Required By default, no simple text authentication key is configured
Configure an MD5/SM3 authentication key	**ip ospf** [*ip-address*] **message-digest-key** *key-id* {**md5 | sm3}** { **0 | 7** } *password*	Required By default, no MD5/SM3 authentication key is configured
Configure key-chain authentication	**ip ospf** [*ip-address*] **key-chain** *key-chain name*	Required By default, the **key-chain** authentication is not configured

41.2.5 Configure OSPF Route Generation *-S -E -A*

In OSPF, direct network segment routes are overwritten by the **network** command, and external routes can be Re-distributed or host routes can be added by the **host** command.

Configuration Conditions

Before configuring OSPF route generation, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible;
- Enable OSPF protocol.

Configure OSPF Route Re-distribution

When multiple routing protocols run on a single device and the routes from other protocols are introduced to OSPF through Re-distribution. An OSPF type 2 external route is generated by default with a metric value of 20. When introducing an external route by Re-distribution, you can modify the external route type, metric and Tag fields and configure the corresponding route policy for route control and management.

Table 41-12 Configure OSPF Route Re-distribution

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF route Re-distribution	**redistribute** *protocol* [*protocol-id*] [**metric** *metric-value* / **metric-type** *metric-type* / **tag** *tag-value* / **route-map** *route-map-name* / **match** *route-type*]	Required By default, OSPF route Re-distribution is not configured.
Configure the metric value of an OSPF external route	**default-metric** *metric-value*	Optional
Configure the maximum number of external routes Re-distributed by OSPF	**redistribute maximum-prefix maximum-prefix-value [threshold-value [warning-only] / warning-only]**	Optional By default, OSPF has no maximum number of external routes Re-distributed

NOTE

- When the **redistribute** *protocol* [*protocol-id*] **metric** and **default-metric** are configured simultaneously to set the metric value of the external route, the former has higher priority.

Configure OSPF Default Route

After configuring the OSPF Stub and the complete NSSA, a Type-3 default route is automatically generated. The NSSA does not automatically generate a default route. A Type-7 default route can be introduced to NSSA through the command **area** *area-id* **nssa default-information-originate**.

OSPF cannot introduce a Type-5 default route through the **redistribute** command; if necessary, it can be done by configuring the **default-information forward [always]** command.

Table 41-13 Configure OSPF Default Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF to introduce the default route	**default-information originate** [**always** / **metric** *metric-value* / **metric-type** *metric-type* / **route-map** *route-map-name*]	Required By default, the external default route will not be introduced to OSPFAS The introduced default route has the default metric 1 and the external type 2 **always** means that the default route is forced to be generated into the OSPFAS, otherwise, it can be generated only a default route is available in the local routing table

Configure OSPF Host Route

Table 41-14 Configure OSPF Host Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF host route	**host** *ip-address* **area** *area-id* [**cost** *cost*]	Required

Steps	Command	Description
		By default, the host route is not generated

41.2.6 Configure OSPF Route Control *-S -E -A*

Configuration Conditions

Before configuring OSPF route control, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible;
- Enable OSPF protocol.

Configure OSPF Inter-area Route Summary

In OSPF, when ABR advertises other areas of the inter-area routes, each route is advertised separately as a Type-3 LSA. To reduce the size of the OSPF database, you can use the inter-area route summary function to summarize a number of consecutive network segments in the area into a single route and only advertise the summarized routes.

Table 41-15 Configure OSPF Inter-area Route Summary

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF inter-area route summary	**area** *area-id* **range** *ip-address/mask-length* [**advertise** [**cost** *cost*] | **cost** *cost* | **not-advertise**]	Required By default, ABR does not summarize the inter-area routes

NOTE

- The OSPF inter-area route summary function only works on ABR.
- By default, the minimum cost value of the detailed routes is selected as the cost value of the route summary.

Configure OSPF External Route Summary

When OSPF Re-distributes external routes, each route is advertised separately in the external link state advertisements. To reduce the size of the OSPF database, you can use the external route summary function to summarize a number of consecutive network segments outside AS into a single route and only advertise the summarized routes.

After configuring the command **summary-address** on ASBR, you can summarize Type-5 LSA and Type-7 LSA in the summary address range.

Table 41-16 Configure OSPF external route summary

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF external route summary	**summary-address** *ip-address mask* [**not-advertise** | **tag** *tag-value*]	Required By default, ASBR does not summarize the external routes

NOTE

- The OSPF external route summary function only works on ASBR.

Configure OSPF Inter-area Route Filtration

ABR uses ACL or prefix-list for filtration in the in direction when receiving the inter-area routes and uses ACL or prefix-list for filtration in the out direction when advertising the inter-area routes.

Table 41-17 Configure OSPF Inter-area Route Filtration

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF inter-area route filtration	**area** *area-id* **filter-list** { **access** { *access-list-name* | *access-list-number* } | **prefix** *prefix-list-name* } { **in** | **out** }	Required By default, ABR does not filter the inter-area routes

NOTE

- Only standard ACL is supported when matching ACL filtration.
- The OSPF inter-area route filtration function only works on ABR.

Configure OSPF External Route Filtration

Configure the external route filtration, i.e. use ACL or prefix-list to enable or disable flooding of routes outside the OSPF AS into the OSPF AS.

Table 41-18 Configure OSPF External Route Filtration

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure a distribute-list to filter external routes	**distribute-list** { *access-list-name* | *access-list-number* | **prefix** *prefix-list-name* } **out** [*routing-protocol* [*process-id*]]	Required By default, ASBR does not filter the external routes

NOTE

- Only standard ACL is supported when matching ACL filtration.
- The OSPF external route filtration function only works on ASBR.

Configure OSPF Route Installation Filtration

After OSPF calculates the routes through LSA, the calculated OSPF route information can be filtered to prevent some routes from being added to the routing table.

There are three filtration methods:

- Filter the destination address of the route with ACL and prefix-list based on the prefix filtration;
- Filter the next hop of the route with prefix-list based on the next hop filtration. Filter the destination address and next hop of the route with prefix-list;
- Filter the routes based on the route policy.

Table 41-19 Configure OSPF Route Installation Filtration

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF to disable the route installation	**distribute-list** { *access-list-name* | *access-lsit-number* | **gateway** *prefix-list-name1* | **prefix** *prefix-list-name2* [**gateway** *prefix-list-name3*] | **route-map** *route-map-name* } **in** [*interface-name*]	Required By default, the installed route will not be filtered

NOTE

- The configured **prefix**, **gateway and route-map** filtrations are mutually exclusive with the configured ACL. For example, ACL filtration cannot be configured after configuration of the **prefix** filtration.
- The configured **route-map** and **prefix** filtrations are mutually exclusive with the configured **gateway** filtration.
- The configured **prefix** filtration overwrites the configured **gateway** filtration.

Configure the Cost Value of OSPF Interface

By default, the OSPF interface overhead is calculated by reference bandwidth/interface bandwidth.

Table 41-20 Configure the Cost Value of OSPF Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the cost value of OSPF interface	**ip ospf** [*ip-address*] **cost** *cost-value*	Optional By default, it is calculated by reference bandwidth/interface bandwidth.

Configure OSPF Reference Bandwidth

The interface reference bandwidth is mainly used to calculate the interface cost value, 100Mbit/s by default. The OSPF interface cost is calculated by reference bandwidth/interface bandwidth. When the calculated result is greater than 1, the integer part is taken; if it's less than 1, it's 1. Therefore, in networks with bandwidth higher than 100Mbit/s, the optimal route will not be selected correctly. It can be solved by configuring an appropriate reference bandwidth with the **auto-cost reference-bandwidth** command.

Table 41-21 Configure OSPF Reference Bandwidth

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF interface reference bandwidth	**auto-cost reference-bandwidth** *reference-bandwidth*	Optional By default, the reference bandwidth is 100Mbit/s

Configure the Administrative Distance of OSPF

The administrative distance is used to indicate the reliability of the routing protocol. After learning the routes to the same destination network from different routing protocols, the routes with a small administrative distance are selected with priority.

Table 41-22 Configure the Administrative Distance of OSPF

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure the administrative distance of OSPF	**distance** { *distance* [*ip-address wildcard-mask*] [*access-list-name* | *access-list-number*] | **ospf** { **external** *distance* | **inter-area** *distance* | **intra-area** *distance* } }	Optional By default, the administrative distance of OSPF intra-area routes and inter-area routes is 110 and of external routes is 150

Configure the Maximum Number of OSPF Load Balancing Entries

If there are multiple equivalent paths to the same destination address, load balancing is formed, which can improve the utilization rate of link and reduce the burden of link.

Table 41-23 Configure the Maximum Number of OSPF Load Balancing Entries

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure the maximum number of OSPF load balancing entries	**maximum-path** *max-number*	Optional By default, the maximum number of OSPF load balancing entries is 4

Configure the Compatible RFC1583 of OSPF

When there are multiple paths to ASBR or an external route forwarding address, RFC1583 and RFC2328 define different routing rules. When the configuration is compatible with RFC1583, an intra-area path or inter-area path of the backbone area is preferred. When not compatible with RFC1583, an intra-area path of the non-backbone area is preferred.

Table 41-24 Configure the Compatible RFC1583 of OSPF

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure the compatible RFC1583 of OSPF	**compatible rfc1583**	Required By default, RFC1583 is incompatible.

NOTE

- In OSPF AS, the routing rules for all devices need to be consistent, i.e. all or none configurations are compatible with RFC1583 to prevent the formation of a routing loop.

41.2.7 Configure OSPF Network Optimization -S -E -A

Configuration Conditions

Before configuring OSPF network optimization, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible;
- Enable OSPF protocol.

Configure OSPF Neighbor Keepalive Time

The OSPF Hello packet is used to establish and keep alive the neighborship. The default send interval of the Hello packet is determined by the network type. The default send interval of Hello packet is 10s in the Broadcast Networks and P2P and is 30s in P2MP and NBMA.

The neighbor dead interval is used to judge the validity of the neighbor. The default is 4 times the Hello interval. If the OSPF device does not receive the neighbor Hello message after the neighbor dead interval timeout, it believes that the neighbor has been invalid and actively deletes the neighbor.

Table 41-25 Configure OSPF Neighbor Keepalive Time

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF Hello interval	**ip ospf** [*ip-address*] **hello-interval** *interval-value*	Optional The default value, determined according to the network type, is 10s for the Broadcast Networks and P2P and 30s for P2MP and NBMA
Configure OSPF neighbor dead interval	**ip ospf** [*ip-address*] **dead-interval** *interval-value*	Optional The default is 4 times the Hello interval

NOTE

- The Hello interval and neighbor dead interval between neighbor OSPF devices must be consistent, otherwise the neighborship cannot be established.
- When you modify the Hello interval, if the current neighbor dead interval is 4 times the Hello interval, the neighbor dead interval will also be automatically modified to maintain at 4 times; if the current neighbor dead interval is not 4 times the Hello interval, the neighbor dead interval remains unchanged.
- Modifying the dead interval does not affect the Hello interval.

Configure a Passive OSPF Interface

Passive Interface is adopted in the dynamic routing protocol to effectively reduce the consumption of network bandwidth by the routing protocol. An OSPF passive interface can be configured to advertise the route of the direct network segment where the interface is located through the **network** command, but suppress the receiving and sending of OSPF protocol packets on the interface.

Table 41-26 Configure a Passive OSPF Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure a passive OSPF interface	**passive-interface** { *interface-name* [*ip-address*] | **default** }	Required By default, no passive OSPF interface is configured

Configure OSPF Demand Circuit

On P2P and P2MP links, to reduce the line cost, an OSPF demand circuit can be configured to suppress the periodic sending of Hello packet and the periodic refresh of LSA packet. It is mainly used in charged link such as ISDN, SVC and X.25.

Table 41-27 Configure OSPF Demand Circuit

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-

Steps	Command	Description
Configure OSPF demand circuit	**ip ospf** [*ip-address*] **demand-circuit**	Required By default, the OSPF demand circuit is disabled

Configure OSPF Interface Priority

The interface priority is mainly used for the election of DR (Designated Router) and BDR (Backup Designated Router) in Broadcast Networks and NBMA, with the value range from 0 to 255. The higher the value, the higher the priority, 1 by default.

DR and BDR are elected by all devices in the same network segment according to interface priority and Router ID via Hello packet. The rules are as follows:

- The device with the highest priority is elected as DR and the device with the second highest priority is elected as BDR. Devices with the priority of 0 are not involved in election;
- If the interface priority is the same, the device with the highest Router ID is elected as DR, and the device with the second highest Router ID is elected as BDR;
- When DR is invalidated, the BDR immediately becomes DR and a new BDR is elected.

Table 41-28 Configure OSPF Interface Priority

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF interface priority	**ip ospf priority** *priority-value*	Optional By default, the OSPF interface priority is 1

NOTE

- Priorities only affect the election process. When DR and BDR have been elected in the network, the change of interface priority will not affect the election results, only the next DR or BDR election results; so DR is not necessarily the device with the highest interface priority, and BDR is not necessarily the device with the second highest interface priority.

Configure OSPF Interface MTU

When encapsulating OSPF packet, in order to avoid fragmentation, the packet size is limited to be less than or equal to the interface MTU value. When the neighbor devices of OSPF interact the DD packet, they will check whether the MTU is the same by default. Otherwise, the adjacency relation cannot be formed. After OSPF is configured to ignore the interface MTU check, the adjacency relation can be established even if the MTU is different.

Table 41-29 Configure OSPF Interface MTU

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF interface MTU	**ip ospf mtu** *mtu-value*	Optional
Configure OSPF interface to ignore the MTU consistency check	**ip ospf** [*ip-address*] **mtu-ignore**	Required By default, MTU is performed Consistency check

Configure OSPF Interface LSA Transmit Delay

The LSA transmit delay represents the time it takes for the LSA to flood to other devices, and the device sending the LSA will extend the interface transmit time to the aging time of the LSA to be sent. By default, the aging time increases by 1 when a flooded LSA passes through a device. The LSA transmit delay can be configured according to the network condition, with the value range of 1 ~ 840. It is generally used on low speed links.

Table 41-30 Configure OSPF Interface LSA Transmit Delay

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF interface LSA transmit delay	**ip ospf transmit-delay** *delay-value*	Optional By default, the LSA transmit delay is 1s.

Configure OSPF LSA Retransmit

OSPF adopts an acknowledgement mechanism to ensure the data interaction reliability. When an LSA floods on the device interface, the LSA will be added to the retransmit list of the neighbor. If an acknowledgment message is not received from the neighbor after the retransmit interval timeout, the LSA will be retransmitted until an acknowledgment message is received.

Table 41-31 Configure OSPF LSA Retransmit

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF LSA retransmit interval	**ip ospf retransmit-interval** *interval-value*	Optional By default, the retransmit interval is 5s.

Configure OSPF to Disable LSA Diffusion

In some cases in the actual network application, a redundant link is used between OSPF neighbors to reduce the diffusion of OSPF update over the redundant link.

Table 41-32 Configure OSPF to Disable LSA Diffusion

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPF to disable diffusion LS-UPD	**ip ospf database-filter all out**	Required By default, OSPF interface does not disable LSA diffusion.

NOTE

- Configuring OSPF to disable LSA diffusion may cause some route information to be lost.

Configure OSPF SPF Computation Time

The route needs to be recomputed when the OSPF network topology changes. When the network is constantly changing, frequent routing computation will occupy a lot of system resources. By adjusting the time parameter of SPF, the consumption of system resources caused by frequent changes of network is restrained.

Table 41-33 Configure OSPF SPF computation time

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF SPF computation time	**timers throttle spf** *delay-time hold-time max-time*	Optional By default, delay-time is 5000ms, hold-time is 10000ms and max-time is 10000ms

NOTE

- The parameter *delay-time* represents the initial computation delay, *hold-time* represents the hold time, and *max-time* represents the maximum latency for two SPF computations. In the case of infrequent network changes, the interval of continuous routing computation is reduced to *delay-time*. In the case of frequent network changes, it can be adjusted accordingly and increased by *hold-time*×2^{n-2} (n is continuous routing computation times). The latency is extended according to the configured *hold-time* to a maximum of *max-time*.

Configure OSPF Database Overflow

The OSPF database overflow is used to restrict the limit the number of Type-5 LSA in the database.

Table 41-34 Configure OSPF Database Overflow

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-

Steps	Command	Description
Configure OSPF database overflow	**overflow database external** *max-number seconds*	Required By default, the OSPF database overflow function is disabled

NOTE

- After the database overflow is enabled, the database in the OSPF area may be different and some routes may be lost.

41.2.8 Configure OSPF to Link with BFD *-E -A*

Configuration Conditions

Before configuring OSPF to link with BFD, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible;
- Enable OSPF protocol.

Configure OSPF to Link with BFD

BFD provides a method for quickly detecting the state of the line between two devices. When BFD detection is enabled between two neighbor OSPF devices, if there is a line fault between the devices, BFD will quickly detect the fault and notify OSPF protocol, trigger OSPF for routing computation and switch to the backup line to achieve quick route switching.

Table 41-35 Configure OSPF to Link with BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the OSPF specified interface to enable or disable BFD	**ip ospf bfd** [*ip-address* | **disable**]	Required By default, BFD function is disabled
Enter global configuration mode	**exit**	-

Steps	Command	Description
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure all interfaces of the OSPF process to enable BFD	**bfd all-interface**	Optional

NOTE

- When BFD is configured in both OSPF configuration mode and interface configuration mode, the priority of configuration under interface is higher.

41.2.9 Configure OSPF GR *-S -E -A*

GR (Graceful Restart) is used to keep the route information at the forwarding level of the local device and neighbor device unchanged and the forwarding not affected during the master-backup switching; after the device switching and re-running, the two devices synchronize the route information at the protocol level and update the forward layer, so as to achieve the purpose of uninterrupted data forwarding during the switching process.

There are two roles in the GR process:

- GR Restarter end - a device that performs protocol GR.
- GR Helper end - a device that helps the protocol GR.

Distributed devices can serve as GR Restarter and GR Helper, while centralized devices can only serve as GR Helper to assist the Restarter end to complete GR.

Configuration Conditions

Before configuring OSPF GR, ensure that:

- The IP address of the interface is configured to make the adjacent nodes accessible.
- Enable OSPF protocol.

Configure OSPF GR Restarter

Table 41-36 Configure OSPF GR Restarter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-

Steps	Command	Description
Configure OSPF GR	**nsf ietf**	Required By default, the GR function is disabled The function is enabled and the protocol shall support Opaque-LSA. By default, Opaque-LSA is supported.
Configure OSPF GR period	**nsf interval** *grace-period*	Optional By default, the GR period is 95s

NOTE

- The OSPF GR is enabled only in the stack environment or dual master environment.

Configure OSPF GR Helper

The GR Helper helps the Restarter complete GR. By default, the device enables the function and the command **nsf ietf helper disable** is used to disable GR Helper. The command **nsf ietf helper strict-lsa-checking** is used to configure the Helper to strictly check LSA in GR process. If checking any change in LSA, exit GR Helper mode.

Table 41-37 Configure OSPF GR Helper

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPF configuration mode	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF GR Helper	**nsf ietf helper** [**disable** | **strict-lsa-checking**]	Optional By default, the Helper is enabled and LSA will not be checked strictly

41.2.10 OSPF Monitoring and Maintaining *-S -E -A*

Table 41-38 OSPF Monitoring and Maintaining

Command	Description
clear ip ospf [*process-id*] **process**	Reset the OSPF process
clear ip ospf *process-id* **neighbor** *neighbor-ip-address* [*neighbor-router-id*]	Reset the OSPF neighbor
clear ip ospf statistics [*interface-name*]	Clear the OSPF protocol statistics
clear ip ospf [*process-id*] **redistribution**	Readvertise the external route
clear ip ospf [*process-id*] **route**	Recompute the OSPF route
show ip ospf [*process-id*]	Show the basic information about OSPF
show ip ospf [*process-id*] **border-routers**	Show the information on the router to the border device in OSPF
show ip ospf [*process-id*] **buffers**	Show the OSPF packet receiving and sending buffer
show ip ospf [*process-id*] **database** [**adv-router** *router-id* **|** **age** *lsa_age* | **database-summary | max-age |** [**asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | self-originate | summary**] [[*link-state-id*] [**adv-router** *advertising-router-id*] | **self-originate | summary**]]	Show the information about the OSPF database
show ip ospf interface [*interface-name* [**detail**]]	Show the OSPF interface information
show ip ospf [*process-id*] **neighbor** [*neighbor-id* | **all | detail** [**all**] | **interface** *ip-address* [**detail**] | **statistic**]	Show the information about the OSPF neighbor
show ip ospf [*process-id*] **route** [*ip-address mask* | *ip-address/mask-length* |	Show the information about the OSPF protocol route

Command	Description
external | **inter-area** | **intra-area** | **statistic**]	
show ip ospf [*process-id*] **virtual-links**	Show the information about the OSPF virtual link
show ip ospf [*process-id*] **sham-links**	Show the information about the configured OSPF sham link interface, including interface status, cost value and neighbor state

41.3 OSPF Typical Configuration Example

41.3.1 Configure Basic Functions of OSPF *-S -E -A*

Network Requirements

- All devices are configured with OSPF protocol and are divided into Area 0, Area 1 and Area 2. Once configured, all devices can learn the route from each other.
- On back-to-back Ethernet interfaces, the OSPF interface network type can be changed to point-to-point in order to accelerate OSPF neighbor establishment. the interface network type of Area 2 is changed to point-to-point. Once configured, all devices can learn the route from each other.

Network Topology

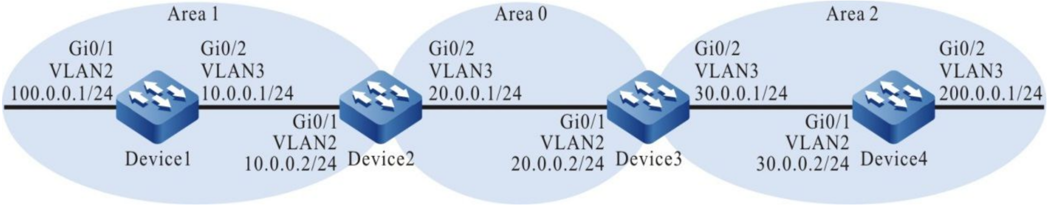


Figure 41-1 Networking for Configuring the Basic Functions of OSPF

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF process and overwrite corresponding interfaces into different areas.

#Configure Device1, configure OSPF process and overwrite the interface into area 1.

```
Device1#configure terminal
```

```
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#Configure Device2, configure OSPF process and overwrite corresponding interfaces into areas 0 and 1.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#Configure Device3, configure OSPF process and overwrite corresponding interfaces into areas 0 and 2.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#Configure Device4, configure OSPF process and overwrite the interface into area 2.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 200.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

NOTE

- Router ID can be manually configured or automatically generated. If Router ID is not manually configured, the device will automatically select a Router ID. First, the device selects the largest IP address in the Loopback interface as the Router ID; if the device is not configured with a Loopback interface address, it will select the large IP address in the ordinary interfaces as the Router ID. Only when the interface is in the up state can the interface address be selected as the Router ID.
- When using the **network** command, the wildcard mask may not exactly match the mask length of the interface IP address, as long as the **network** segment covers the interface IP address. For example, **network 0.0.0.0 255.255.255.255** means covering all interfaces.

#Query the OSPF neighbor information and routing table of Device1.

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State          Dead Time   Address        Interface
2.2.2.2          1    Full/DR        00:00:36    10.0.0.2       vlan3

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 02:26:21, vlan3
O   20.0.0.0/24 [110/2] via 10.0.0.2, 02:25:36, vlan3
O   30.0.0.0/24 [110/3] via 10.0.0.2, 02:25:36, vlan3
C   100.0.0.0/24 is directly connected, 2:26:23 AM, vlan2
C   127.0.0.0/8 is directly connected, 6:09:44 PM, lo0
O   200.0.0.0/24 [110/4] via 10.0.0.2, 02:25:36, vlan3
```

#Query the OSPF neighbor and routing table of Device2.

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State          Dead Time   Address        Interface
1.1.1.1          1    Full/Backup     00:00:37    10.0.0.1       vlan2
3.3.3.3          1    Full/DR        12:00:38 AM    20.0.0.2       vlan3

Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 2:31:15 AM, vlan2
C   20.0.0.0/24 is directly connected, 2:31:50 AM, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 2:31:40 AM, vlan3
O   100.0.0.0/24 [110/2] via 10.0.0.1, 2:30:29 AM, vlan2
C   127.0.0.0/8 is directly connected, 240:21:34, lo0
O   200.0.0.0/24 [110/3] via 20.0.0.2, 2:31:40 AM, vlan3
```

#Query OSPF LSDB (link state database) of Device2.

```
Device2#show ip ospf database

            OSPF Router with ID (2.2.2.2) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age Seq#       CkSum  Link count
2.2.2.2         2.2.2.2         1777 0x8000000c 0xcb20 1
3.3.3.3         3.3.3.3          309 0x8000000a 0x9153 1

                Net Link States (Area 0)

Link ID         ADV Router      Age Seq#       CkSum
20.0.0.2        3.3.3.3          369 0x80000006 0xec12

                Summary Link States (Area 0)

Link ID         ADV Router      Age Seq#       CkSum  Route
10.0.0.0        2.2.2.2         1757 0x80000005 0xcc59 10.0.0.0/24
100.0.0.0       2.2.2.2         1356 0x80000005 0x408a 100.0.0.0/24
30.0.0.0        3.3.3.3            9 0x80000006 0xa765 30.0.0.0/24
200.0.0.0       3.3.3.3          149 0x80000006 0x075a 200.0.0.0/24

                Router Link States (Area 1)

Link ID         ADV Router      Age Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         1775 0x80000009 0xbbda 2
2.2.2.2         2.2.2.2         1737 0x80000008 0x2dd5 1

                Net Link States (Area 1)

Link ID         ADV Router      Age Seq#       CkSum
10.0.0.2        2.2.2.2           34 0x80000006 0x39db

                Summary Link States (Area 1)

Link ID         ADV Router      Age Seq#       CkSum  Route
20.0.0.0        2.2.2.2          144 0x80000006 0x48d2 20.0.0.0/24
30.0.0.0        2.2.2.2         1186 0x80000005 0xd13f 30.0.0.0/24
200.0.0.0       2.2.2.2           14 0x80000006 0x2f35 200.0.0.0/24
```

For Device2, 30.0.0.0/24 and 200.0.0.0/24 are inter-area routes. The LSA information of relevant routes can be queried from Summary Link States (Area 0) and of intra-area routes may be queried only by **show ip ospf database router**.

Step 4: Configure OSPF interface network type to P2P.

#Configure Device3 and change OSPF network type of the interface VLAN3 to P2P.

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip ospf network point-to-point
Device3(config-if-vlan3)#exit
```

#Configure Device4 and change OSPF network type of the interface VLAN2 to P2P.

```
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ip ospf network point-to-point
Device4(config-if-vlan2)#exit
```

Step 5: Check the result.

#Query the OSPF neighbor and routing table of Device3.

```
Device3#show ip ospf neighbor
OSPF process 100:
Neighbor ID    Pri   State          Dead Time   Address       Interface
2.2.2.2         1    Full/Backup    12:00:36 AM    20.0.0.1      vlan2
4.4.4.4         1    Full/ -        00:00:39    30.0.0.2      vlan3

Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set


O   10.0.0.0/24 [110/2] via 20.0.0.1, 12:02:53 AM, vlan2
C   20.0.0.0/24 is directly connected, 3:20:36 AM, vlan2
C   30.0.0.0/24 is directly connected, 3:20:26 AM, vlan3
O   100.0.0.0/24 [110/3] via 20.0.0.1, 12:01:51 AM, vlan2
C   127.0.0.0/8 is directly connected, 262:1:24 AM, lo0
O   200.0.0.0/24 [110/2] via 30.0.0.2, 12:00:11 AM, vlan3
```

NOTE

- DR and BDR will not be elected when a P2P establishes OSPF adjacency.

#Query the OSPF neighbor and routing table of Device4.

```
Device4#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   Full/ -         00:00:39    30.0.0.1        vlan2

Device4#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   10.0.0.0/24 [110/3] via 30.0.0.1, 12:01:04 AM, vlan2
O   20.0.0.0/24 [110/2] via 30.0.0.1, 12:01:04 AM, vlan2
C   30.0.0.0/24 is directly connected, 3:20:25 AM, vlan2
O   100.0.0.0/24 [110/4] via 30.0.0.1, 12:01:04 AM, vlan2
C   127.0.0.0/8 is directly connected, 10:52:36 PM, lo0
C   200.0.0.0/24 is directly connected, 3:20:13 AM, vlan3
```

As you can see, after modifying the OSPF interface network type to P2P, a neighbor can be established normally and can learn the route normally.

NOTE

- When the OSPF interface network type is configured, the OSPF interface network type at both ends of the neighbor must be consistent, otherwise, it will affect the normal learning and flooding of the route. By default, the OSPF interface network type is determined by the network type of the physical interface.

41.3.2 Configure OSPF Authentication *-S -E -A*

Network Requirements

- All devices run OSPF and configure the area authentication. Area 0 is configured for simple text authentication, and Area 1 for MD5 authentication.
- Configure OSPF interface authentication. The interface authentication of Area 0 is configured as simple text authentication and of Area 1 is configured as MD5 authentication.
- After configuration, the devices can establish a neighbor normally and learn the routes from each other.

Network Topology

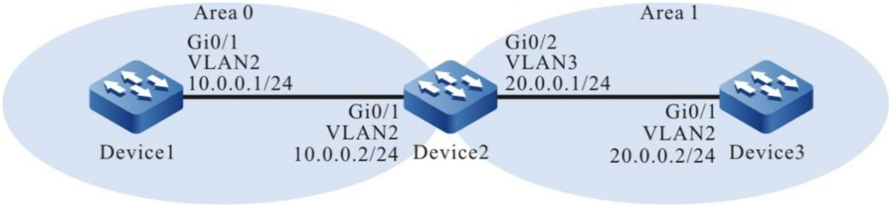


Figure 41-2 Networking for Configuring the OSPF Authentication

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF process, overwrite the corresponding interface into different areas and enable area authentication. Area 0 uses simple text authentication and Area 1 uses MD5 authentication.

#Configure Device1, OSPF process and area authentication function.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 0 authentication
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2, OSPF process and area authentication function.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 0 authentication
Device2(config-ospf)#area 1 authentication message-digest
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#Configure Device3, OSPF process and area authentication function.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#area 1 authentication message-digest
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 1
Device3(config-ospf)#exit
```

#Query the OSPF process information of Device1.

```
Device1#show ip ospf 100
 Routing Process "ospf 100" with ID 1.1.1.1
 Process bound to VRF default
 Process uptime is 30 minutes
 IETF NSF restarter support disabled
 IETF NSF helper support enabled
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA is 0
 External LSA database is unlimited.
 Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
 Number of areas attached to this router: 1
   Area 0 (BACKBONE)        Number of interfaces in this area is 1(1)
      Number of fully adjacent neighbors in this area is 1
      Number of fully adjacent sham-link neighbors in this area is 0
      Area has simple password authentication
      SPF algorithm last executed 00:27:43.916 ago
      SPF algorithm executed 3 times
      Number of LSA 4. Checksum Sum 0x0160f7
      Not Support Demand Circuit lsa number is 0,
      Indication lsa (by other routers) number is: 0,
      Area support flood DoNotAge Lsa
```

As you can see, the area authentication is simple text authentication.

#Query the OSPF neighbor information and routing table of Device1.

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   Full/DR        12:00:38 AM    10.0.0.2        vlan2


Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:14:01 AM, vlan2
O   20.0.0.0/24 [110/2] via 10.0.0.2, 12:10:38 AM, vlan2
C   127.0.0.0/8 is directly connected, 8:55:08 PM, lo0
```

On Device1, the neighbor is normally established and the route is learnt normally.

#Query the OSPF process information of Device3.

```
Device3#show ip ospf 100
 Routing Process "ospf 100" with ID 3.3.3.3
 Process bound to VRF default
 Process uptime is 28 minutes
 IETF NSF restarter support disabled
 IETF NSF helper support enabled
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA is 0
 External LSA database is unlimited.
 Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
 Number of areas attached to this router: 1
   Area 1        Number of interfaces in this area is 1(1)
      Number of fully adjacent neighbors in this area is 1
      Number of fully adjacent sham-link neighbors in this area is 0
      Number of fully adjacent virtual neighbors through this area is 0
      Area has message digest authentication
      SPF algorithm last executed 12:24:01 AM.783 ago
      SPF algorithm executed 5 times
      Number of LSA 4. Checksum Sum 0x0337cf
      Not Support Demand Circuit lsa number is 0,
      Indication lsa (by other routers) number is: 0,
      Area support flood DoNotAge Lsa
```

As you can see, the area authentication is MD5 authentication.

#Query the OSPF neighbor information and routing table of Device3.

```
Device3#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State          Dead Time   Address        Interface
2.2.2.2          1   Full/Backup     12:00:33 AM    20.0.0.1       vlan2

Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   10.0.0.0/24 [110/2] via 20.0.0.1, 12:09:31 AM, vlan2
C   20.0.0.0/24 is directly connected, 12:20:36 AM, vlan2
C   127.0.0.0/8 is directly connected, 24:12:06 AM, lo0
```

On Device3, the neighbor is normally established and the route is learnt normally.

Step 4:   Configure OSPF interface authentication.

#Configure Device1 and use the simple text authentication for the interface VLAN2, with the password of admin.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf authentication
Device1(config-if-vlan2)#ip ospf authentication-key 0 admin
Device1(config-if-vlan2)#exit
```

#Configure Device2 and use the simple text authentication for the interface VLAN2, with the password of admin; use MD5 authentication for the interface VLAN3, with the Key ID of 1 and the password of admin.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip ospf authentication
Device2(config-if-vlan2)#ip ospf authentication-key 0 admin
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip ospf authentication message-digest
Device2(config-if-vlan3)#ip ospf message-digest-key 1 md5 0 admin
Device2(config-if-vlan3)#exit
```

#Configure Device3 and use MD5 authentication for the interface VLAN2, with the Key ID of 1 and the password of admin.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip ospf authentication message-digest
```

```
Device3(config-if-vlan2)#ip ospf message-digest-key 1 md5 0 admin
Device3(config-if-vlan2)#exit
```

Step 5: Check the result.

#Query the OSPF neighbor information of Device2.

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State          Dead Time   Address        Interface
1.1.1.1          1   Full/Backup     12:00:33 AM    10.0.0.1        vlan2
3.3.3.3          1   Full/DR        12:00:39 AM    20.0.0.2       vlan3
```

#Query the OSPF interface information of Device2.

```
Device2#show ip ospf interface vlan2
vlan2 is up, line protocol is up
  Internet Address 10.0.0.2, 10.0.0.255( a[10.0.0.2] d[10.0.0.255]) Area 0, MTU 1500
  Process ID 100, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, TE Metric 0
  Designated Router (ID) 2.2.2.2, Interface Address 10.0.0.2
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.0.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 0
  Graceful restart proxy id is 0x0
  Hello received 406 sent 454, DD received 8 sent 6
  LS-Req received 2 sent 2, LS-Upd received 11(LSA: 15) sent 10(LSA: 14)
  LS-Ack received 10 sent 0, Discarded 0

Device2#show ip ospf interface vlan3
vlan3 is up, line protocol is up
  Internet Address 20.0.0.1, 20.0.0.255( a[20.0.0.1] d[20.0.0.255]) Area 1, MTU 1500
  Process ID 100, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 0
  Designated Router (ID) 3.3.3.3, Interface Address 20.0.0.2
  Backup Designated Router (ID) 2.2.2.2, Interface Address 20.0.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 12:00:00 AM
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 485
  Graceful restart proxy id is 0x0
```

```
Hello received 412 sent 454, DD received 9 sent 12
LS-Req received 3 sent 3, LS-Upd received 9(LSA: 10) sent 13(LSA: 16)
LS-Ack received 13 sent 8, Discarded 0
```

The authentication sequence number (Crypt Sequence Number) will be generated after configuration of the MD5 authentication and will not be generated in the simple text authentication.

NOTE

- When configuring OSPF authentication, you can configure only area authentication or only interface authentication, or you can configure both area authentication and interface authentication.
- When the area authentication and interface authentication are configured simultaneously, the interface authentication takes precedence.

41.3.3 Configure OSPF Route Re-distribution *-S -E -A*

Network Requirements

- Run OSPF between Device1 and Device2, and run RIPv2 between Device2 and Device3.
- Device2 Re-distributes the RIP route to OSPF and uses a route policy to control that only the route 100.0.0.0/24 is Re-distributed.

Network Topology

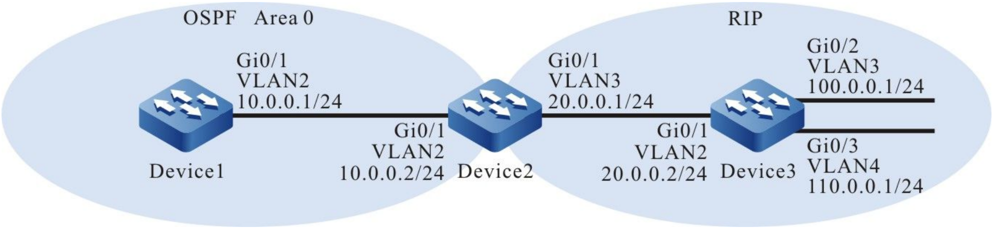


Figure 41-3 Networking for Configuring OSPF to Re-distribute Routes

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF between Device 1 and Device 2; configure RIPv2 between Device2 and Device 3.

#Configure OSPF of Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure OSPF and RIPv2 of Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 20.0.0.0
Device2(config-rip)#exit
```

#Configure RIPv2 of Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 20.0.0.0
Device3(config-rip)#network 100.0.0.0
Device3(config-rip)#network 110.0.0.0
Device3(config-rip)#exit
```

#Query the OSPF neighbor information of Device1.

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State          Dead Time   Address        Interface
2.2.2.2          1   Full/DR        12:00:32 AM    10.0.0.2       vlan2
```

#Query the OSPF neighbor information of Device2.

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State          Dead Time   Address        Interface
1.1.1.1          1   Full/Backup     12:00:32 AM    10.0.0.1       vlan2
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

```
C   10.0.0.0/24 is directly connected, 12:21:17 AM, vlan2
C   20.0.0.0/24 is directly connected, 12:21:33 AM, vlan3
R   100.0.0.0/24 [120/1] via 20.0.0.2, 00:10:58, vlan3
R   110.0.0.0/24 [120/1] via 20.0.0.2, 00:10:58, vlan3
C   127.0.0.0/8 is directly connected, 30:8:17 PM, lo0
```

On Device2, the RIP route is learnt.

Step 4: Configure the route policy.

#Configure Device2.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map RIPtoOSPF
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#exit
```

Configure route-map to invoke ACL to match 100.0.0.0/24 only and filter the other network segments, such as 20.0.0.0/24 and 110.0.0.0/24.

Step 5: Configure OSPF to re-distribute RIP routes and associate a route policy.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip route-map RIPtoOSPF
Device2(config-ospf)#exit
```

When redistributing RIP routes, revoke the route-map matching rule for filtration.

Step 6: Check the result.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
     D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


C   10.0.0.0/24 is directly connected, 12:47:27 AM, vlan2
OE  100.0.0.0/24 [150/20] via 10.0.0.2, 00:21:39, vlan2
C   127.0.0.0/8 is directly connected, 9:40:06 PM, lo0
```

Only OSPF external route 100.0.0.0/24 is learnt from the routing table of Device1 and the routes 20.0.0.0/24 and 110.0.0.0/24 are filtered.

#Query the OSPF process information of Device2.

```
Device2#show ip ospf 100
 Routing Process "ospf 100" with ID 2.2.2.2
 Process bound to VRF default
 Process uptime is 1 hour 4 minutes
 IETF NSF restarter support disabled
 IETF NSF helper support enabled
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ASBR (injecting external routing information)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Refresh timer 10 secs
 Number of external LSA 2. Checksum Sum 0x0161F5
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of non-default external LSA is 2
 External LSA database is unlimited.
 Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
 Number of areas attached to this router: 1
   Area 0 (BACKBONE)        Number of interfaces in this area is 1(1)
       Number of fully adjacent neighbors in this area is 1
       Number of fully adjacent sham-link neighbors in this area is 0
       Area has no authentication
       SPF algorithm last executed 12:37:52 AM.833 ago
       SPF algorithm executed 3 times
       Number of LSA 3. Checksum Sum 0x00e746
       Not Support Demand Circuit lsa number is 0,
       Indication lsa (by other routers) number is: 0,
       Area support flood DoNotAge Lsa

Device2#show ip ospf 100 database


            OSPF Router with ID (2.2.2.2) (Process ID 100)


                Router Link States (Area 0)


Link ID         ADV Router       Age Seq#       CkSum  Link count
```

```
1.1.1.1        1.1.1.1        191 0x80000004 0x70a0 1
2.2.2.2        2.2.2.2        537 0x80000005 0x36ce 1

               Net Link States (Area 0)

Link ID        ADV Router     Age Seq#       CkSum
10.0.0.2        2.2.2.2        818 0x80000003 0x3fd8

               AS External Link States

Link ID        ADV Router     Age Seq#       CkSum  Route
100.0.0.0       2.2.2.2        718 0x80000002 0x72be E2 100.0.0.0/24  [0x0]
```

From the OSPF 100 process information, the role of Device2 has become the ASBR, and only an external LSA has been generated in the database.

NOTE

- In an actual application, if there are two or more AS boundary routers, it is recommended that you do not Re-distribute routes between different routing protocols. If route Re-distribution must be configured, you are required to configure routing policies to prevent routing loops.

41.3.4 Configure OSPF Multiple Processes *-S -E -A*

Network Requirements

- Run the OSPF protocol on all devices and enable two OSPF processes on Device2; establish a neighbor of OSPF 100 process on Device1 and Device2; establish a neighbor of OSPF 200 process on Device3 and Device2.
- Two OSPF processes on Device2 Re-distribute routes to each other. The OSPF 100 process Re-distributes only the route 110.0.0.0/24 using the route policy; the OSPF 200 process Re-distributes only the route 100.0.0.0/24 using the route policy.

Network Topology

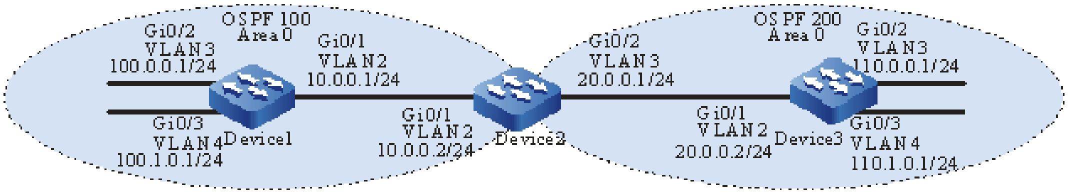


Figure 41-4 Networking for Configuring the OSPF Multiple Processes

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.1.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2 and create two OSPF processes, process 100 and process 200.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router ospf 200
Device2(config-ospf)#router-id 2.2.2.3
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 200
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 110.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 110.1.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

NOTE

- When there are multiple OSPF processes, it is recommended to configure different Router IDs among OSPF processes to avoid the hidden danger of Router ID conflict.

#Query LSDB and neighbor information of Device2.

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   Full/Backup     12:00:30 AM    10.0.0.1        vlan2
OSPF process 200:
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   Full/DR        12:00:33 AM    20.0.0.2        vlan3

Device2#show ip ospf database

          OSPF Router with ID (2.2.2.2) (Process ID 100)

             Router Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          19 0x80000016 0x53bf 3
2.2.2.2         2.2.2.2          15 0x80000010 0x1ae1 1

             Net Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum
10.0.0.2         2.2.2.2          21 0x80000001 0x43d6

          OSPF Router with ID (2.2.2.3) (Process ID 200)

             Router Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum  Link count
2.2.2.3         2.2.2.3          14 0x8000000f 0xb235 1
3.3.3.3         3.3.3.3          15 0x8000001b 0x696b 3

             Net Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum
20.0.0.2         3.3.3.3          15 0x80000002 0x03fe
```

The OSPF process 100 and process 200 of Device2 have adjacency relation and separate OSPF databases.

#Query the OSPF routing table of Device2.

```
Device2#show ip ospf route
OSPF process 100:
```

```
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.0.0.0/24 [1] is directly connected, vlan2, Area 0
O  100.0.0.0/24 [2] via 10.0.0.1, vlan2, Area 0
O  100.1.0.0/24 [2] via 10.0.0.1, vlan2, Area 0
OSPF process 200:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  20.0.0.0/24 [1] is directly connected, vlan3, Area 0
O  110.0.0.0/24 [2] via 20.0.0.2, vlan3, Area 0
O  110.1.0.0/24 [2] via 20.0.0.2, vlan3, Area 0
```

The OSPF process 100 and the OSPF process 200 calculate their respective routes.

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C    10.0.0.0/24 is directly connected, 12:05:34 AM, vlan2
C    20.0.0.0/24 is directly connected, 12:05:28 AM, vlan3
O    100.0.0.0/24 [110/2] via 10.0.0.1, 12:04:42 AM, vlan2
O    100.1.0.0/24 [110/2] via 10.0.0.1, 12:04:42 AM, vlan2
O    110.0.0.0/24 [110/2] via 20.0.0.2, 12:04:41 AM, vlan3
O    110.1.0.0/24 [110/2] via 20.0.0.2, 12:04:41 AM, vlan3
C    127.0.0.0/8 is directly connected, 48:40:33, lo0
```

Step 4:   Configure the route policy.

#Configure Device2.

```
Device2(config)#ip prefix-list 1 permit 110.0.0.0/24
Device2(config)#ip prefix-list 2 permit 100.0.0.0/24
Device2(config)#route-map OSPF200to100
Device2(config-route-map)#match ip address prefix-list 1
Device2(config-route-map)#exit
```

```
Device2(config)#route-map OSPF100to200
Device2(config-route-map)#match ip address prefix-list 2
Device2(config-route-map)#exit
```

Configure route-map to revoke prefix-list1 and 2 to match the network segments 110.0.0.0/24 and 100.0.0.0/24.

NOTE

- In configuring a route policy, you can create a filtration rule based on a prefix list or ACL. The prefix list can precisely match routing masks while the ACL cannot match routing masks.

Step 5: Configure OSPF processes to Re-distribute routes to each other and associate a route policy.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute ospf 200 route-map OSPF200to100
Device2(config-ospf)#exit
Device2(config)#router ospf 200
Device2(config-ospf)#redistribute ospf 100 route-map OSPF100to200
Device2(config-ospf)#exit
```

Step 6: Check the result.

#Query OSPF LSDB of Device2.

```
Device2#show ip ospf database

      OSPF Router with ID (2.2.2.2) (Process ID 100)

        Router Link States (Area 0)

Link ID      ADV Router     Age Seq#      CkSum  Link count
1.1.1.1      1.1.1.1       1663 0x80000016 0x53bf 3
2.2.2.2      2.2.2.2        216 0x80000011 0x1eda 1

        Net Link States (Area 0)

Link ID      ADV Router     Age Seq#      CkSum
```

```
10.0.0.2        2.2.2.2         1664 0x80000001 0x43d6

                AS External Link States

Link ID         ADV Router      Age Seq#        CkSum  Route
110.0.0.0       2.2.2.2         216 0x80000001 0x3dfc E2 110.0.0.0/24  [0x0]

            OSPF Router with ID (2.2.2.3) (Process ID 200)

                Router Link States (Area 0)


Link ID         ADV Router      Age Seq#        CkSum  Link count
2.2.2.3         2.2.2.3         205 0x80000010 0xb62e 1
3.3.3.3         3.3.3.3         1658 0x8000001b 0x696b 3

                Net Link States (Area 0)

Link ID         ADV Router      Age Seq#        CkSum
20.0.0.2        3.3.3.3         1658 0x80000002 0x03fe

                AS External Link States

Link ID         ADV Router      Age Seq#        CkSum  Route
100.0.0.0       2.2.2.3         205 0x80000001 0xb989 E2 100.0.0.0/24  [0x0]
```

It can be seen that the OSPF process 100 only has the LSA of the external route 110.0.0.0/24, and the other routes 110.1.0.0/24 and 20.0.0.0/24 are filtered by the route policy OSPF200to100; similarly, the OSPF process 200 only has the LSA of the external route 100.0.0.0/24, and the other routes 100.1.0.0/24 and 10.0.0.0/24 are filtered by the route policy OSPF100to200.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:40:20 AM, vlan2
C   100.0.0.0/24 is directly connected, 3:11:36 AM, vlan3
C   100.1.0.0/24 is directly connected, 1:00:22 AM, vlan4
OE  110.0.0.0/24 [150/2] via 10.0.0.2, 12:15:27 AM, vlan2
C   127.0.0.0/8 is directly connected, 97:8:23 AM, lo0
```

Device1 only learns the route 110.0.0.0/24.

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   20.0.0.0/24 is directly connected, 12:42:44 AM, vlan2
OE  100.0.0.0/24 [150/2] via 20.0.0.1, 12:17:45 AM, vlan2
C   110.0.0.0/24 is directly connected, 1:02:03 AM, vlan3
C   110.1.0.0/24 is directly connected, 1:02:14 AM, vlan4
C   127.0.0.0/8 is directly connected, 41:2:01 AM, lo0
```

Device3 only learns the route 100.0.0.0/24.

NOTE

- In an actual application, if there are two or more AS boundary routers, it is recommended that you do not Re-distribute routes between different OSPF processes. If route Re-distribution must be configured, you are required to configure route filtration policies to prevent routing loops.

41.3.5 Configure OSPF External Route Summary *-S -E -A*

Network Requirements

- Run OSPF between Device1 and Device2, and run RIPv2 between Device2 and Device3.
- Device2 Re-distributes RIP routes to OSPF. To reduce the number of routes on Device1, the Re-distributed RIP routes are summarized as 20.0.0.0/16 on ASBR.

Network Topology

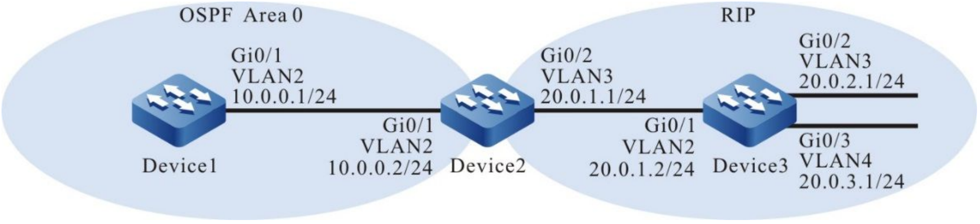


Figure 41-5 Networking for Configuring OSPF External Route Summary

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF and RIPv2.

#Configure OSPF of Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure OSPF and RIPv2 of Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 20.0.0.0
Device2(config-rip)#exit
```

#Configure RIPv2 of Device3.

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 20.0.0.0
Device3(config-rip)#exit
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:15:46 AM, vlan2
C   20.0.1.0/24 is directly connected, 12:15:23 AM, vlan3
R   20.0.2.0/24 [120/1] via 20.0.1.2, 12:12:17 AM, vlan3
R   20.0.3.0/24 [120/1] via 20.0.1.2, 12:12:06 AM, vlan3
C   127.0.0.0/8 is directly connected, 3:34:27 AM, lo0
```

Step 4: Configure OSPF to re-distribute RIP routes.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip
Device2(config-ospf)#exit
```

#Query OSPF LSDB of Device2.

```
Device2#show ip ospf database

      OSPF Router with ID (2.2.2.2) (Process ID 100)

        Router Link States (Area 0)

Link ID      ADV Router      Age Seq#      CkSum  Link count
1.1.1.1      1.1.1.1        1071 0x80000003 0x729f 1
2.2.2.2      2.2.2.2         873 0x80000004 0x38cd 1

        Net Link States (Area 0)

Link ID      ADV Router      Age Seq#      CkSum
10.0.0.2      2.2.2.2        1070 0x80000001 0x43d6

        AS External Link States

Link ID      ADV Router      Age Seq#      CkSum  Route
20.0.1.0      2.2.2.2         365 0x80000001 0x7d04 E2 20.0.1.0/24  [0x0]
20.0.2.0      2.2.2.2         365 0x80000001 0x720e E2 20.0.2.0/24  [0x0]
20.0.3.0      2.2.2.2         365 0x80000001 0x6718 E2 20.0.3.0/24  [0x0]
```

As you can see from the OSPF database, three external LSAs have been generated, indicating that the RIP routes have been Re-distributed to OSPF.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:56:40 AM, vlan2
```

```
OE  20.0.1.0/24 [150/20] via 10.0.0.2, 12:02:40 AM, vlan2
OE  20.0.2.0/24 [150/20] via 10.0.0.2, 12:02:40 AM, vlan2
OE  20.0.3.0/24 [150/20] via 10.0.0.2, 12:02:40 AM, vlan2
C   127.0.0.0/8 is directly connected, 115:12:28 PM, lo0
```

Device1 learns the Re-distributed RIP routes.

Step 5: Configure the OSPF external route summary on ASBR. At this point, Device2 is ASBR.

#Configure Device2 and summarize the Re-distributed RIP routes as 20.0.0.0/16.

```
Device2(config)#router ospf 100
Device2(config-ospf)#summary-address 20.0.0.0 255.255.0.0
Device2(config-ospf)#exit
```

Step 6: Check the result.

#Query OSPF LSDB of Device2.

```
Device2#show ip ospf database

            OSPF Router with ID (2.2.2.2) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         1437 0x80000003 0x729f 1
2.2.2.2         2.2.2.2         1240 0x80000004 0x38cd 1

                Net Link States (Area 0)

Link ID         ADV Router      Age Seq#       CkSum
10.0.0.2         2.2.2.2          144 0x80000002 0x41d7

                AS External Link States

Link ID         ADV Router      Age Seq#       CkSum  Route
20.0.0.0         2.2.2.2           84 0x80000001 0x88f9 E2 20.0.0.0/16  [0x0]
```

According to step 3, three external LSAs originally generated in the database have been deleted, and a summarized external LSA has been regenerated.

#Query the routing table of Device2.

```
Device2#show ip route
```

```
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:28:03 AM, vlan2
O   20.0.0.0/16 [110/1] is directly connected, 00:04:48, null0
C   20.0.1.0/24 is directly connected, 12:27:40 AM, vlan3
R   20.0.2.0/24 [120/1] via 20.0.1.2, 12:24:34 AM, vlan3
R   20.0.3.0/24 [120/1] via 20.0.1.2, 12:24:23 AM, vlan3
C   127.0.0.0/8 is directly connected, 3:46:44 AM, lo0
```

NOTE

- A summary route 20.0.0.0/16 at output interface to Null0 is automatically added to the routing table of Device2 to avoid loops.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:58:40 AM, vlan2
OE  20.0.0.0/16 [150/20] via 10.0.0.2, 12:15:26 AM, vlan2
C   127.0.0.0/8 is directly connected, 115:5:28 PM, lo0
```

Only the summarized route 20.0.0.0/16 is learnt in the routing table of Device1.

41.3.6 Configure OSPF Inter-area Route Summary *-S -E -A*

Network Requirements

- All devices are configured with OSPF protocol and are divided into Area 0 and Area 1.
- To reduce the number of inter-area routes, summarize the inter-area routes on ABR, summarize the routes in Area 0 as 10.0.0.0/16 and the routes in Area 1 as 20.0.0.0/16.

Network Topology

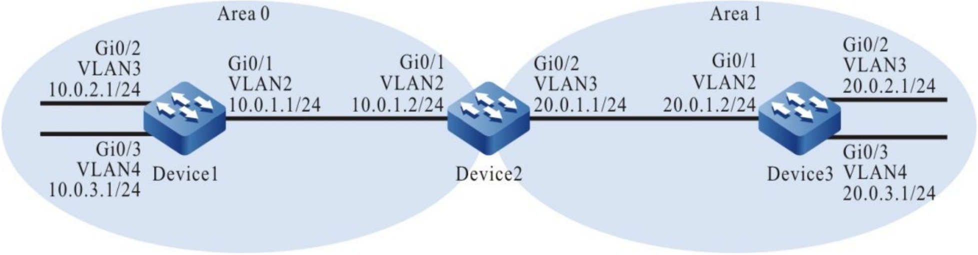


Figure 41-6 Networking for Configuring OSPF Inter-area Route Summary

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF process and overwrite corresponding interfaces into different areas.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.3.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.2.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.3.0 0.0.0.255 area 1
Device3(config-ospf)#exit
```

#Query OSPF LSDB and routing table of Device2.

```
Device2#show ip ospf database
```

```
        OSPF Router with ID (2.2.2.2) (Process ID 100)

          Router Link States (Area 0)

Link ID       ADV Router      Age Seq#      CkSum  Link count
1.1.1.1       1.1.1.1         1419 0x80000007 0x4f81 3
2.2.2.2       2.2.2.2         1414 0x80000004 0x4bb9 1

          Net Link States (Area 0)

Link ID       ADV Router      Age Seq#      CkSum
10.0.1.2       2.2.2.2         1419 0x80000001 0x38e0

          Summary Link States (Area 0)

Link ID       ADV Router      Age Seq#      CkSum  Route
20.0.1.0       2.2.2.2         1437 0x80000001 0x47d7 20.0.1.0/24
20.0.2.0       2.2.2.2         1363 0x80000001 0x46d6 20.0.2.0/24
20.0.3.0       2.2.2.2         1363 0x80000001 0x3be0 20.0.3.0/24

          Router Link States (Area 1)


Link ID       ADV Router      Age Seq#      CkSum  Link count
2.2.2.2       2.2.2.2         1368 0x80000004 0xe70b 1
3.3.3.3       3.3.3.3         1341 0x80000006 0x6138 3

          Net Link States (Area 1)

Link ID       ADV Router      Age Seq#      CkSum
20.0.1.1       2.2.2.2         1368 0x80000001 0x24e3

          Summary Link States (Area 1)

Link ID       ADV Router      Age Seq#      CkSum  Route
10.0.1.0       2.2.2.2         1442 0x80000001 0xc95f 10.0.1.0/24
10.0.2.0       2.2.2.2         1409 0x80000001 0xc85e 10.0.2.0/24
10.0.3.0       2.2.2.2         1409 0x80000001 0xbd68 10.0.3.0/24
```

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.1.0/24 is directly connected, 12:30:31 AM, vlan2
O   10.0.2.0/24 [110/2] via 10.0.1.1, 12:23:37 AM, vlan2
O   10.0.3.0/24 [110/2] via 10.0.1.1, 12:23:37 AM, vlan2
C   20.0.1.0/24 is directly connected, 2:09:10 AM, vlan3
O   20.0.2.0/24 [110/2] via 20.0.1.2, 12:22:51 AM, vlan3
O   20.0.3.0/24 [110/2] via 20.0.1.2, 12:22:51 AM, vlan3
C   127.0.0.0/8 is directly connected, 5:28:14 AM, lo0
```

Three inter-area LSAs are generated between Area 0 and Area 1 in OSPF database of Device2. The intra-area routes in all areas are also added to the routing table.

#Query OSPF LSDB and routing table of Device1.

```
Device1#show ip ospf database

            OSPF Router with ID (1.1.1.1) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router      Age Seq#        CkSum  Link count
1.1.1.1         1.1.1.1         249 0x80000008 0x4d82 3
2.2.2.2         2.2.2.2         191 0x80000005 0x49ba 1

                Net Link States (Area 0)

Link ID         ADV Router      Age Seq#        CkSum
10.0.1.2        2.2.2.2         471 0x80000002 0x36e1

                Summary Link States (Area 0)

Link ID         ADV Router      Age Seq#        CkSum  Route
20.0.1.0        2.2.2.2         251 0x80000002 0x45d8 20.0.1.0/24
20.0.2.0        2.2.2.2        1988 0x80000001 0x46d6 20.0.2.0/24
20.0.3.0        2.2.2.2        1988 0x80000001 0x3be0 20.0.3.0/24

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.1.0/24 is directly connected, 12:25:11 AM, vlan2
C   10.0.2.0/24 is directly connected, 12:24:58 AM, vlan3
C   10.0.3.0/24 is directly connected, 12:24:44 AM, vlan4
O   20.0.1.0/24 [110/2] via 10.0.1.2, 12:14:59 AM, vlan2
O   20.0.2.0/24 [110/3] via 10.0.1.2, 12:14:12 AM, vlan2
O   20.0.3.0/24 [110/3] via 10.0.1.2, 12:14:12 AM, vlan2
C   127.0.0.0/8 is directly connected, 116:7:42 PM, lo0
```

Three inter-area LSAs in the OSPF database of Device1 are also added to the routing table.

#Query OSPF LSDB and routing table of Device3.

```
Device3#show ip ospf database

       OSPF Router with ID (3.3.3.3) (Process ID 100)

          Router Link States (Area 1)

Link ID        ADV Router      Age Seq#       CkSum  Link count
2.2.2.2        2.2.2.2         532 0x80000005 0xe50c 1
3.3.3.3        3.3.3.3         506 0x80000007 0x5f39 3

          Net Link States (Area 1)

Link ID        ADV Router      Age Seq#       CkSum
20.0.1.1        2.2.2.2         532 0x80000002 0x22e4

          Summary Link States (Area 1)

Link ID        ADV Router      Age Seq#       CkSum  Route
10.0.1.0        2.2.2.2          82 0x80000002 0xc760 10.0.1.0/24
10.0.2.0        2.2.2.2         382 0x80000002 0xc65f 10.0.2.0/24
10.0.3.0        2.2.2.2         262 0x80000002 0xbb69 10.0.3.0/24

Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

```
O   10.0.1.0/24 [110/2] via 20.0.1.1, 12:24:04 AM, vlan2
O   10.0.2.0/24 [110/3] via 20.0.1.1, 12:24:04 AM, vlan2
O   10.0.3.0/24 [110/3] via 20.0.1.1, 12:24:04 AM, vlan2
C   20.0.1.0/24 is directly connected, 2:09:51 AM, vlan2
C   20.0.2.0/24 is directly connected, 2:07:21 AM, vlan3
C   20.0.3.0/24 is directly connected, 2:07:09 AM, vlan4
C   127.0.0.0/8 is directly connected, 360:8:45 PM, lo0
```

Similarly, three inter-area LSAs in the OSPF database of Device3 are also added to the routing table.

Step 4: Configure the inter-area route summary on ABR. At this point, Device2 is ASBR.

#Configure Device2 and summarize the routes in Area 0 as 10.0.0.0/16 and the routes in Area 1 as 20.0.0.0/16.

```
Device2(config)#router ospf 100
Device2(config-ospf)#area 0 range 10.0.0.0/16
Device2(config-ospf)#area 1 range 20.0.0.0/16
Device2(config-ospf)#exit
```

Step 5: Check the result.

#Query OSPF LSDB and routing table of Device2.

```
Device2#show ip ospf database

      OSPF Router with ID (2.2.2.2) (Process ID 100)

        Router Link States (Area 0)

Link ID     ADV Router    Age Seq#      CkSum  Link count
1.1.1.1     1.1.1.1       305 0x80000009 0x4b83 3
2.2.2.2     2.2.2.2       297 0x80000006 0x47bb 1

        Net Link States (Area 0)

Link ID     ADV Router    Age Seq#      CkSum
10.0.1.2     2.2.2.2       527 0x80000003 0x34e2

        Summary Link States (Area 0)

Link ID     ADV Router    Age Seq#      CkSum  Route
20.0.0.0     2.2.2.2        23 0x80000001 0x52cd 20.0.0.0/16
```

```
                Router Link States (Area 1)

Link ID         ADV Router      Age Seq#       CkSum  Link count
2.2.2.2         2.2.2.2         277 0x80000006 0xe30d 1
3.3.3.3         3.3.3.3         332 0x80000008 0x5d3a 3

                Net Link States (Area 1)

Link ID         ADV Router      Age Seq#       CkSum
20.0.1.1        2.2.2.2         317 0x80000003 0x20e5

                Summary Link States (Area 1)

Link ID         ADV Router      Age Seq#       CkSum  Route
10.0.0.0        2.2.2.2          26 0x80000001 0xd455 10.0.0.0/16

Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   10.0.0.0/16 [110/1] is directly connected, 12:00:31 AM, null0
C   10.0.1.0/24 is directly connected, 12:40:31 AM, vlan2
O   10.0.2.0/24 [110/2] via 10.0.1.1, 12:33:37 AM, vlan2
O   10.0.3.0/24 [110/2] via 10.0.1.1, 12:33:37 AM, vlan2
O   20.0.0.0/16 [110/1] is directly connected, 12:00:27 AM, null0
C   20.0.1.0/24 is directly connected, 2:19:10 AM, vlan3
O   20.0.2.0/24 [110/2] via 20.0.1.2, 12:32:51 AM, vlan3
O   20.0.3.0/24 [110/2] via 20.0.1.2, 12:32:51 AM, vlan3
C   127.0.0.0/8 is directly connected, 5:38:14 AM, lo0
```

According to step 2, Area 0 and Area 1 in the OSPF database of Device2 only generate a summarized inter-area LSA. Similarly, a summary route to Null0 interface is automatically added to the routing table.

#Query OSPF LSDB and routing table of Device1.

```
Device1#show ip ospf database


             OSPF Router with ID (1.1.1.1) (Process ID 100)


                Router Link States (Area 0)
```

```
Link ID      ADV Router      Age Seq#      CkSum  Link count
1.1.1.1      1.1.1.1        1338 0x80000009 0x4b83 3
2.2.2.2      2.2.2.2        1332 0x80000006 0x47bb 1

             Net Link States (Area 0)

Link ID      ADV Router      Age Seq#      CkSum
10.0.1.2      2.2.2.2        1563 0x80000003 0x34e2

             Summary Link States (Area 0)

Link ID      ADV Router      Age Seq#      CkSum  Route
20.0.0.0      2.2.2.2          90 0x80000001 0x52cd 20.0.0.0/16

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.1.0/24 is directly connected, 12:40:11 AM, vlan2
C   10.0.2.0/24 is directly connected, 12:39:58 AM, vlan3
C   10.0.3.0/24 is directly connected, 12:39:44 AM, vlan4
O   20.0.0.0/16 [110/2] via 10.0.1.2, 12:02:18 AM, vlan2
C   127.0.0.0/8 is directly connected, 116:44:42, lo0
```

On Device1, only the summarized inter-area LSA exists in OSPF database and only the summarized route 20.0.0.0/16 in the Area 1 is learnt in the routing table; similarly, only the summarized route 10.0.0.0/16 in Area 0 is learnt on Device3.

41.3.7 Configure OSPF Inter-area Route Filtration *-S -E -A*

Network Requirements

- All devices are configured with OSPF protocol and are divided into Area 0 and Area 1.
- Filter the inter-area routes on ABR. In Area 0, the route 20.0.3.0/24 is not allowed to inject and the route 10.0.3.0/24 is allowed to flood to other areas.

Network Topology

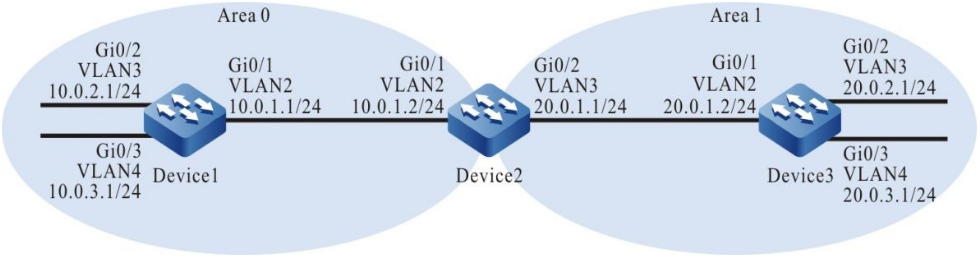


Figure 41-7 Networking for Configuring OSPF Inter-area Route Filtration

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF process and overwrite corresponding interfaces into different areas.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.3.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.2.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.3.0 0.0.0.255 area 1
Device3(config-ospf)#exit
```

#Query OSPF LSDB and routing table of Device2.

```
Device2#show ip ospf database
```

```
          OSPF Router with ID (2.2.2.2) (Process ID 100)

                Router Link States (Area 0)

Link ID       ADV Router      Age Seq#       CkSum  Link count
1.1.1.1       1.1.1.1         329 0x8000005b 0xa6d5 3
2.2.2.2       2.2.2.2         324 0x80000051 0xb007 1

                Net Link States (Area 0)

Link ID       ADV Router      Age Seq#       CkSum
10.0.1.2       2.2.2.2         324 0x8000004e 0x9d2e

                Summary Link States (Area 0)

Link ID       ADV Router      Age Seq#       CkSum  Route
20.0.1.0       2.2.2.2         324 0x8000004e 0xac25 20.0.1.0/24
20.0.2.0       2.2.2.2         324 0x8000004d 0xad23 20.0.2.0/24
20.0.3.0       2.2.2.2         259 0x80000001 0x3be0 20.0.3.0/24

                Router Link States (Area 1)

Link ID       ADV Router      Age Seq#       CkSum  Link count
2.2.2.2       2.2.2.2         334 0x80000055 0x4f51 1
3.3.3.3       3.3.3.3         335 0x80000059 0xca7a 3

                Net Link States (Area 1)

Link ID       ADV Router      Age Seq#       CkSum
20.0.1.2       3.3.3.3         340 0x80000001 0xeb17

                Summary Link States (Area 1)

Link ID       ADV Router      Age Seq#       CkSum  Route
10.0.1.0       2.2.2.2         365 0x80000001 0xc95f 10.0.1.0/24
10.0.2.0       2.2.2.2         319 0x80000001 0xc85e 10.0.2.0/24
10.0.3.0       2.2.2.2         256 0x80000001 0xbd68 10.0.3.0/24

Device2#show ip route
```

```
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.1.0/24 is directly connected, 12:06:13 AM, vlan2
O   10.0.2.0/24 [110/2] via 10.0.1.1, 12:05:22 AM, vlan2
O   10.0.3.0/24 [110/2] via 10.0.1.1, 12:05:22 AM, vlan2
C   20.0.1.0/24 is directly connected, 12:06:19 AM, vlan3
O   20.0.2.0/24 [110/2] via 20.0.1.2, 12:05:32 AM, vlan3
O   20.0.3.0/24 [110/2] via 20.0.1.2, 12:05:32 AM, vlan3
C   127.0.0.0/8 is directly connected, 94:42:22, lo0
```

Three inter-area LSAs are generated between Area 0 and Area 1 in OSPF database of Device2. The intra-area routes are also added to the routing table.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.1.0/24 is directly connected, 12:08:41 AM, vlan2
C   10.0.2.0/24 is directly connected, 37:59:10, vlan3
C   10.0.3.0/24 is directly connected, 38:5:36 AM, vlan4
O   20.0.1.0/24 [110/2] via 10.0.1.2, 12:07:55 AM, vlan2
O   20.0.2.0/24 [110/3] via 10.0.1.2, 12:07:55 AM, vlan2
O   20.0.3.0/24 [110/3] via 10.0.1.2, 12:06:50 AM, vlan2
C   127.0.0.0/8 is directly connected, 70:7:32 AM, lo0
```

Device1 learns the route of Area 1.

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   10.0.1.0/24 [110/2] via 20.0.1.1, 12:08:44 AM, vlan2
O   10.0.2.0/24 [110/3] via 20.0.1.1, 12:08:33 AM, vlan2
O   10.0.3.0/24 [110/3] via 20.0.1.1, 12:07:30 AM, vlan2
C   20.0.1.0/24 is directly connected, 12:09:31 AM, vlan2
```

```
C   20.0.2.0/24 is directly connected, 37:59:57, vlan3
C   20.0.3.0/24 is directly connected, 38:3:35 AM, vlan4
C   127.0.0.0/8 is directly connected, 61:26:38, lo0
```

Device3 learns the route of Area 0.

Step 4: Configure the route filtration policy.

#Configure Device2.

```
Device2(config)#ip prefix-list 1 deny 10.0.3.0/24
Device2(config)#ip prefix-list 1 permit 0.0.0.0/0 le 32
Device2(config)#ip prefix-list 2 deny 20.0.3.0/24
Device2(config)#ip prefix-list 2 permit 0.0.0.0/0 le 32
Device2(config)#exit
```

prefix-list1 filters the network 10.0.3.0/24 and allows all other networks; 2 filters the network 20.0.3.0/24 and allows all other networks.

Step 5: Configure the inter-area path filtration on ABR and invoke the matching rules of prefix-list.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#area 0 filter-list prefix 1 out
Device2(config-ospf)#area 0 filter-list prefix 2 in
Device2(config-ospf)#exit
```

Step 6: Check the result.

#Query OSPF LSDB of Device2.

```
Device2#show ip ospf database

            OSPF Router with ID (2.2.2.2) (Process ID 100)

                Router Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          679 0x8000005b 0xa6d5 3
2.2.2.2         2.2.2.2          673 0x80000051 0xb007 1

                Net Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum
```

```
10.0.1.2        2.2.2.2         673 0x8000004e 0x9d2e


                Summary Link States (Area 0)


Link ID         ADV Router      Age Seq#       CkSum  Route
20.0.1.0        2.2.2.2         673 0x8000004e 0xac25 20.0.1.0/24
20.0.2.0        2.2.2.2         673 0x8000004d 0xad23 20.0.2.0/24


                Router Link States (Area 1)


Link ID         ADV Router      Age Seq#       CkSum  Link count
2.2.2.2         2.2.2.2         683 0x80000055 0x4f51 1
3.3.3.3         3.3.3.3         684 0x80000059 0xca7a 3


                Net Link States (Area 1)


Link ID         ADV Router      Age Seq#       CkSum
20.0.1.2        3.3.3.3         689 0x80000001 0xeb17


                Summary Link States (Area 1)


Link ID         ADV Router      Age Seq#       CkSum  Route
10.0.1.0        2.2.2.2         714 0x80000001 0xc95f 10.0.1.0/24
10.0.2.0        2.2.2.2         668 0x80000001 0xc85e 10.0.2.0/24
```

According to the results of step 2, LSA of the network 20.0.3.0/24 in OSPF database has been deleted from Area 0 and LSA of the network 10.0.3.0/24 has been deleted from Area 1.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


C   10.0.1.0/24 is directly connected, 12:12:57 AM, vlan2
C   10.0.2.0/24 is directly connected, 38:3:25 AM, vlan3
C   10.0.3.0/24 is directly connected, 38:9:52 AM, vlan4
O   20.0.1.0/24 [110/2] via 10.0.1.2, 12:12:11 AM, vlan2
O   20.0.2.0/24 [110/3] via 10.0.1.2, 12:12:11 AM, vlan2
C   127.0.0.0/8 is directly connected, 70:11:48 AM, lo0
```

The route 20.0.3.0/24 no longer exists in the routing table of Device1.

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   10.0.1.0/24 [110/2] via 20.0.1.1, 12:13:09 AM, vlan2
O   10.0.2.0/24 [110/3] via 20.0.1.1, 12:12:58 AM, vlan2
C   20.0.1.0/24 is directly connected, 12:13:56 AM, vlan2
C   20.0.2.0/24 is directly connected, 38:4:22 AM, vlan3
C   20.0.3.0/24 is directly connected, 38:8:00 AM, vlan4
C   127.0.0.0/8 is directly connected, 64:31:03, lo0
```

The route 10.0.3.0/24 no longer exists in the routing table of Device3.

41.3.8 Configure OSPF Complete Stub *-S -E -A*

Network Requirements

- All devices are configured with OSPF protocol and are divided into Area 0, Area 1 and Area 2. Area 1 is a complete Stub.
- On Device4, Re-distribute a static route to OSPF. After configuration, the complete Stub cannot learn the inter-area routes and external routes, and the devices in the other areas can learn the inter-area routes and external routes.

Network Topology

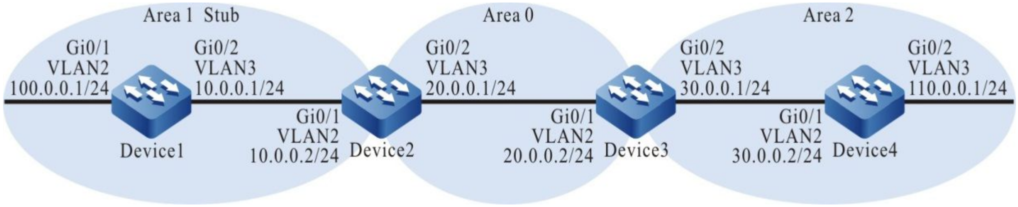


Figure 41-8 Networking for Configuring OSPF Complete Stub

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF process and overwrite corresponding interfaces into corresponding areas.

#Configure Device1 and configure area 1 to Stub.

```
Device1#configure terminal
```

```
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 1 stub
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#Configure Device2 and configure area 1 to complete Stub. Device2 is ABR and no-summary can take effect only on ABR.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 stub no-summary
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 110.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

Step 4: Device4 configures a static route and re-distributes it to OSPF.

#Configure Device4.

```
Device4(config)#ip route 200.1.1.0 255.255.255.0 110.0.0.2
Device4(config)#router ospf 100
Device4(config-ospf)#redistribute static
Device4(config-ospf)#exit
```

Step 5: Check the result.

#Query OSPF LSDB and routing table of Device1.

```
Device1#show ip ospf database


      OSPF Router with ID (1.1.1.1) (Process ID 100)


        Router Link States (Area 1 [Stub])


Link ID     ADV Router     Age Seq#      CkSum  Link count
1.1.1.1     1.1.1.1        19 0x80000009 0x8513 2
2.2.2.2     2.2.2.2        22 0x80000005 0x51b6 1


        Net Link States (Area 1 [Stub])


Link ID     ADV Router     Age Seq#      CkSum
10.0.0.2     2.2.2.2        22 0x80000001 0x61ba


        Summary Link States (Area 1 [Stub])


Link ID     ADV Router     Age Seq#      CkSum  Route
0.0.0.0     2.2.2.2        55 0x80000002 0x73c1 0.0.0.0/0


Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is 10.0.0.2 to network 0.0.0.0


O   0.0.0.0/0 [110/2] via 10.0.0.2, 12:00:19 AM, vlan3
C   10.0.0.0/24 is directly connected, 12:01:04 AM, vlan3
C   100.0.0.0/24 is directly connected, 12:11:55 AM, vlan2
C   127.0.0.0/8 is directly connected, 30:46:57, lo0
```

From OSPF database, there is no inter-area LSA or external route LSA except for an inter-area LSA 0.0.0.0/0 in area 1. ABR in the Stub will generate an inter-area route 0.0.0.0/0, which is flooded in the complete Stub. The data going out of the area and out of AS are all forwarded relying on this default route.

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:01:02 AM, vlan2
C   20.0.0.0/24 is directly connected, 12:00:59 AM, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 12:00:17 AM, vlan3
O   100.0.0.0/24 [110/2] via 10.0.0.1, 12:00:10 AM, vlan2
O   110.0.0.0/24 [110/3] via 20.0.0.2, 12:00:17 AM, vlan3
C   127.0.0.0/8 is directly connected, 56:7:04 AM, lo0
OE  200.1.1.0/24 [150/20] via 20.0.0.2, 12:00:16 AM, vlan3
```

As you can see, Device2 can learn the inter-area route and external route.

NOTE

- Only when the command **area** *area-id* **stub** is configured on ABR in Stub without adding **no-summary** can the devices in the area learn the inter-area routes rather than external routes. The devices can access the network outside AS through the default route.

41.3.9 Configure OSPF NSSA Area *-S -E -A*

Network Requirements

- All devices are configured with OSPF protocol and are divided into Area 0, Area 1 and Area 2. Area 1 and Area 2 are NSSA areas.
- On Device4, Re-distribute a static route to OSPF. After configuration, all devices can learn the intra-area and inter-area routes, but the external routes cannot be injected into Area 1.
- Introduce a default route to ABR in Area 1, so that Device1 can access the external network through the default route.

Network Topology

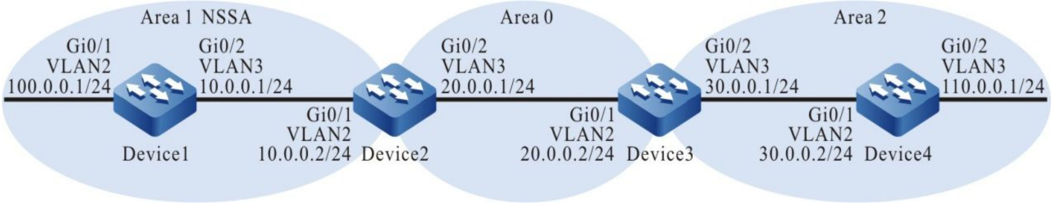


Figure 41-9 Networking for Configuring OSPF NSSA

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF process and overwrite corresponding interfaces into corresponding areas.

#Configure Device1 and configure area 1 to NSSA area.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 1 nssa
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#Configure Device2 and configure area 1 to NSSA area.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 nssa
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3 and configure area 2 to NSSA area.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#area 2 nssa
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#Configure Device4 and configure area 2 to NSSA area.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#area 2 nssa
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 110.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

Step 4: Device4 configures a static route and re-distributes it to OSPF.

#Configure Device4.

```
Device4(config)#ip route 200.1.1.0 255.255.255.0 110.0.0.2
Device4(config)#router ospf 100
Device4(config-ospf)#redistribute static
Device4(config-ospf)#exit
```

#Query OSPF LSDB of Device3.

```
Device3#show ip ospf database

      OSPF Router with ID (3.3.3.3) (Process ID 100)

        Router Link States (Area 0)

Link ID      ADV Router      Age Seq#      CkSum  Link count
2.2.2.2      2.2.2.2         179 0x80000004 0xe110 1
3.3.3.3      3.3.3.3         177 0x80000004 0xa345 1

        Net Link States (Area 0)

Link ID      ADV Router      Age Seq#      CkSum
20.0.0.2      3.3.3.3         182 0x80000001 0xf60d

        Summary Link States (Area 0)

Link ID      ADV Router      Age Seq#      CkSum  Route
10.0.0.0      2.2.2.2         214 0x80000001 0xd455 10.0.0.0/24
100.0.0.0      2.2.2.2         173 0x80000001 0x4886 100.0.0.0/24
30.0.0.0      3.3.3.3         208 0x80000001 0xb160 30.0.0.0/24
110.0.0.0      3.3.3.3         171 0x80000001 0xa719 110.0.0.0/24

        ASBR-Summary Link States (Area 0)

Link ID      ADV Router      Age Seq#      CkSum
4.4.4.4      3.3.3.3         171 0x80000001 0x72ac

        Router Link States (Area 2 [NSSA])

Link ID      ADV Router      Age Seq#      CkSum  Link count
3.3.3.3      3.3.3.3         175 0x80000004 0x686f 1
4.4.4.4      4.4.4.4         177 0x80000005 0xe46a 2
```

```
              Net Link States (Area 2 [NSSA])

Link ID        ADV Router      Age Seq#       CkSum
30.0.0.2        4.4.4.4         177 0x80000001 0xc827

              Summary Link States (Area 2 [NSSA])

Link ID        ADV Router      Age Seq#       CkSum  Route
10.0.0.0        3.3.3.3         172 0x80000001 0xde48 10.0.0.0/24
20.0.0.0        3.3.3.3         214 0x80000001 0x52cb 20.0.0.0/24
100.0.0.0       3.3.3.3          172 0x80000001 0x5279 100.0.0.0/24

              NSSA-external Link States (Area 2 [NSSA])


Link ID        ADV Router      Age Seq#       CkSum  Route
200.1.1.0       4.4.4.4          247 0x80000001 0x6cde N2 200.1.1.0/24 [0x0]

              AS External Link States

Link ID        ADV Router      Age Seq#       CkSum  Route
200.1.1.0       3.3.3.3          176 0x80000001 0x0156 E2 200.1.1.0/24  [0x0]
```

From OSPF database, ABR in NSSA (area 2) will convert NSSA-external LSA to AS External LSA, so the other areas can normally learn the external routes Re-distributed from NSSA (area 2)

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:02:53 AM, vlan2
C   20.0.0.0/24 is directly connected, 12:02:51 AM, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 12:02:04 AM, vlan3
O   100.0.0.0/24 [110/2] via 10.0.0.1, 12:02:04 AM, vlan2
O   110.0.0.0/24 [110/3] via 20.0.0.2, 12:02:02 AM, vlan3
C   127.0.0.0/8 is directly connected, 6:47:22 AM, lo0
OE  200.1.1.0/24 [150/20] via 20.0.0.2, 12:02:02 AM, vlan3
```

Device2 has learnt the external routes Re-distributed from NSSA (area 2).

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
     D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.0.0.0/24 is directly connected, 12:02:29 AM, vlan3
O   20.0.0.0/24 [110/2] via 10.0.0.2, 12:01:44 AM, vlan3
O   30.0.0.0/24 [110/3] via 10.0.0.2, 12:01:41 AM, vlan3
C   100.0.0.0/24 is directly connected, 1:53:00 AM, vlan2
O   110.0.0.0/24 [110/4] via 10.0.0.2, 12:01:40 AM, vlan3
C   127.0.0.0/8 is directly connected, 383:45:55, lo0
```

As you can see, route 200.1.1.0/24 does not exist in the Device1 routing table, indicating that the external routes Re-distributed from Device4 have not been injected into NSSA (area 1), and other inter-area routes have been added to the routing table.

Step 5:   Configure Device2 and introduce the default route to area 1.

#Configure Device2. At this point, Device2 is ABR of area 1.

```
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 nssa default-information-originate
Device2(config-ospf)#exit
```

NOTE

- After the command **area** *area-id* **nssa no-summary** is configured on ABR in NSSA area, the area is also called complete NSSA. At this point, ABR also generates a default route and floods it into NSSA; after this command is configured, it can further reduce the summary LSA and the corresponding inter-area routes. Access the networks outside the area and AS through this default route.

Step 6:   Check the result.

#Query OSPF LSDB of Device2.

```
Device2#show ip ospf database

            OSPF Router with ID (2.2.2.2) (Process ID 100)

              Router Link States (Area 0)
```

```
Link ID         ADV Router       Age Seq#       CkSum  Link count
2.2.2.2         2.2.2.2          455 0x80000004 0xe110 1
3.3.3.3         3.3.3.3          455 0x80000004 0xa345 1

                Net Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum
20.0.0.2         3.3.3.3          461 0x80000001 0xf60d

                Summary Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum  Route
10.0.0.0         2.2.2.2          492 0x80000001 0xd455 10.0.0.0/24
100.0.0.0         2.2.2.2          449 0x80000001 0x4886 100.0.0.0/24
30.0.0.0         3.3.3.3          487 0x80000001 0xb160 30.0.0.0/24
110.0.0.0        3.3.3.3          449 0x80000001 0xa719 110.0.0.0/24

                ASBR-Summary Link States (Area 0)

Link ID         ADV Router       Age Seq#       CkSum
4.4.4.4         3.3.3.3          449 0x80000001 0x72ac

                Router Link States (Area 1 [NSSA])

Link ID         ADV Router       Age Seq#       CkSum  Link count
1.1.1.1         1.1.1.1          456 0x80000005 0x8d0f 2
2.2.2.2         2.2.2.2          457 0x80000004 0x59ad 1

                Net Link States (Area 1 [NSSA])

Link ID         ADV Router       Age Seq#       CkSum
10.0.0.2         2.2.2.2          457 0x80000001 0x61ba

                Summary Link States (Area 1 [NSSA])

Link ID         ADV Router       Age Seq#       CkSum  Route
20.0.0.0         2.2.2.2          492 0x80000001 0x70b1 20.0.0.0/24
30.0.0.0         2.2.2.2          449 0x80000001 0xf71f 30.0.0.0/24
110.0.0.0        2.2.2.2          448 0x80000001 0xedd7 110.0.0.0/24
```

```
                NSSA-external Link States (Area 1 [NSSA])



Link ID         ADV Router      Age Seq#       CkSum  Route
0.0.0.0         2.2.2.2          31 0x80000001 0x5b42 N2 0.0.0.0/0 [0x0]


                AS External Link States


Link ID         ADV Router      Age Seq#       CkSum  Route
200.1.1.0        3.3.3.3         454 0x80000001 0x0156 E2 200.1.1.0/24  [0x0]
```

OSPF generates an NSSA-external LSA for the default route.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


OE  0.0.0.0/0 [150/1] via 10.0.0.2, 12:00:22 AM, vlan3
C   10.0.0.0/24 is directly connected, 12:07:29 AM, vlan3
O   20.0.0.0/24 [110/2] via 10.0.0.2, 12:06:44 AM, vlan3
O   30.0.0.0/24 [110/3] via 10.0.0.2, 12:06:41 AM, vlan3
C   100.0.0.0/24 is directly connected, 1:58:00 AM, vlan2
O   110.0.0.0/24 [110/4] via 10.0.0.2, 12:06:40 AM, vlan3
C   127.0.0.0/8 is directly connected, 383:50:55, lo0
```

The default route 0.0.0.0/0 is learnt from the routing table of Device1 and used for communication with the AS external routes.

41.3.10 Configure OSPF to Link with BFD *-E -A*

Network Requirements

- All devices are configured with OSPF protocol.
- The line between Device1 and Device3 enables BFD detection function. When a fault occurs in the line, BFD will quickly detect the fault and inform OSPF. OSPF switches the route to Device2 for communication.

Network Topology

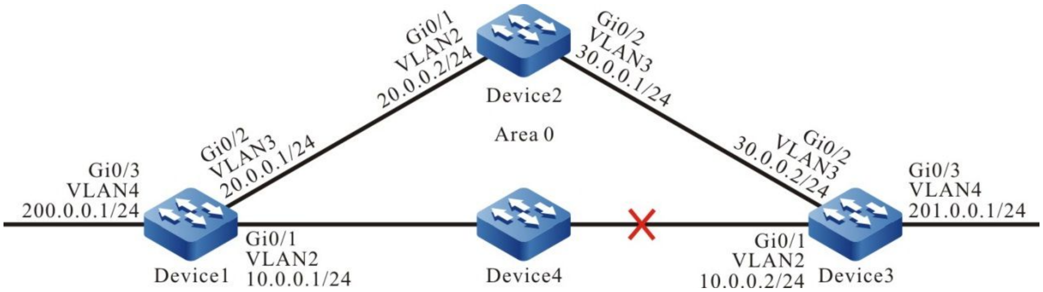


Figure 41-10 Networking for Configuring OSPF to Link with BFD

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure the OSPF process.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

Step 4: Configure OSPF to link with BFD.

#Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf bfd
Device1(config-if-vlan2)#exit
```

#Configure Device3.

```
Device3(config)#bfd fast-detect
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip ospf bfd
Device3(config-if-vlan2)#exit
```

Step 5: Check the result.

#Query the OSPF neighbor information and routing table of Device1.

```
Device1#show ip ospf neighbor 3.3.3.3

OSPF process 100:
 Neighbor 3.3.3.3, interface address 10.0.0.2
   In the area 0 via interface vlan2, BFD enabled
   Neighbor priority is 1, State is Full, 5 state changes
   DR is 10.0.0.2, BDR is 10.0.0.1
   Options is 0x42 (-|O|-|-|-|-|E|-)
   Dead timer due in 00:00:31
   Neighbor is up for 00:02:46
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
   Crypt Sequence Number is 0
   Graceful restart proxy id is 0x0
   Thread Inactivity Timer on
   Thread Database Description Retransmission off, 0 times
   Thread Link State Request Retransmission off, 0 times
   Thread Link State Update Retransmission off, 0 times

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set


C   10.0.0.0/24 is directly connected, 12:01:09 AM, vlan2

C   20.0.0.0/24 is directly connected, 12:55:37 AM, vlan3

O   30.0.0.0/24 [110/2] via 20.0.0.2, 12:02:50 AM, vlan3

              [110/2] via 10.0.0.2, 00:01:30, vlan2

C   127.0.0.0/8 is directly connected, 5:51:09 AM, lo0

C   200.0.0.0/24 is directly connected, 12:55:12 AM, vlan4

O   201.0.0.0/24 [110/2] via 10.0.0.2, 12:01:30 AM, vlan2
```

It can be seen from the OSPF neighbor information that BFD has been enabled and the route 201.0.0.0/24 prefers the line between Device1 and Device3 for communication.

#Query the BFD session of Device1.

```
Device1#show bfd session detail

Total session number: 1

OurAddr            NeighAddr          LD/RD          State        Holddown      interface

10.0.0.1           10.0.0.2           7/14           UP           5000          vlan2

Type:direct

Local State:UP  Remote State:UP  Up for: 0h:2m:37s  Number of times UP:1

Send Interval:1000ms  Detection time:5000ms(1000ms*5)

Local Diag:0  Demand mode:0  Poll bit:0

MinTxInt:1000  MinRxInt:1000  Multiplier:5

Remote MinTxInt:1000  Remote MinRxInt:1000  Remote Multiplier:5

Registered protocols:OSPF
```

It can be seen that OSPF coordinates with BFD successfully and the session is established normally.

#After a fault occurs in the line between Device1 and Device3, BFD will quickly detect the fault and inform OSPF. OSPF switches the route to Device2 for communication. Query the routing table of Device1.

```
   %BFD-5-Session [10.0.0.2,10.0.0.1,vlan2,10] DOWN (Detection time expired)

   %OSPF-5-ADJCHG: Process 100 Nbr [vlan2:10.0.0.1-3.3.3.3] from Full to Down,KillNbr: BFD session
down


   Device1#show ip route

   Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management

          D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


   Gateway of last resort is not set


   C   10.0.0.0/24 is directly connected, 12:01:59 AM, vlan2

   C   20.0.0.0/24 is directly connected, 12:56:13 AM, vlan3

   O   30.0.0.0/24 [110/2] via 20.0.0.2, 12:03:40 AM, vlan3
```

```
C   127.0.0.0/8 is directly connected, 5:52:41 AM, lo0
C   200.0.0.0/24 is directly connected, 12:56:02 AM, vlan4
O   201.0.0.0/24 [110/3] via 20.0.0.2, 12:00:06 AM, vlan3
```

Device3 behaves similarly to Device1.

42 OSPFv3

42.1 Overview

OSPFv3, as the short name of version 3 of OSPF (Open Shortest Path First), mainly provides support for IPv6, complies with RFC2328 and RFC2740 and supports other OSPF extensions as defined by the RFC.

OSPFv3 has basically the same principle as OSPFv2 and only has some changes for different IP protocols and address families, as follows:

- OSPFv3 runs on the link and OSPFv2 runs on the network segment;
- OSPFv3 supports multiple instances per link;
- OSPFv3 marks the adjacent neighbor by Router ID, and OSPFv2 marks the adjacent neighbor by IP address;

42.2 OSPFv3 Function Configuration

Table 42-1 OSPFv3 Function List

Configuration task	
Configure basic functions of OSPFv3	Enable OSPFv3 protocol
Configure OSPFv3 area	Configure OSPFv3 NSSA area
	Configure OSPFv3 Stub area
	Configure an OSPFv3 virtual link
Configure OSPFv3 network type	Configure OSPFv3 interface network type to broadcast
	Configure OSPFv3 interface network type to P2P
	Configure OSPFv3 interface network type to NBMA
	Configure OSPFv3 interface network type to P2MP

Configuration task	
Configure OSPFv3 network authentication	Configure OSPFv3 area authentication
	Configure OSPFv3 interface authentication
Configure OSPFv3 route generation	Configure OSPFv3 route Re-distribution
	Configure OSPFv3 default route
Configure OSPFv3 route control	Configure OSPFv3 inter-area route summary
	Configure OSPFv3 external route summary
	Configure OSPFv3 inter-area route filtration
	Configure OSPFv3 external route filtration
	Configure OSPFv3 route installation filtration
	Configure the cost value of OSPFv3 interface
	Configure OSPFv3 reference bandwidth
	Configure the administrative distance of OSPFv3
	Configure the maximum number of OSPFv3 load balancing entries
Configure OSPFv3 network optimization	Configure OSPFv3 neighbor Keepalive time
	Configure a passive OSPFv3 interface
	Configure OSPFv3 demand circuit
	Configure OSPFv3 interface priority
	Configure OSPFv3 OSPF interface to ignore MTU

Configuration task	
	Configure OSPFv3 interface LSA transmit delay
	Configure OSPFv3 LSA retransmit
	Configure OSPFv3 SPF computation time
Configure OSPFv3 GR	Configure OSPFv3 GR Restarter
	Configure OSPFv3 GR Helper
Configure OSPFv3 to link with BFD	Configure OSPFv3 to link with BFD

42.2.1 Configure Basic Functions of OSPFv3 *-E -A*

In all OSPFv3 configuration tasks, the OSPFv3 protocol must be enabled before the configuration of other features can take effect.

Configuration Conditions

Before configuring the basic functions of OSPFv3, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- The IPv6 forwarding function is enabled.

Enable OSPFv3 Protocol

To enable OSPFv3, you shall first create an OSPFv3 process, specify the Router ID of the process, and enable the OSPFv3 protocol on the interface.

A device running the OSPFv3 protocol must have a Router ID that uniquely identifies a device within an OSPFv3. It is necessary to ensure the uniqueness of the Router ID in the AS, otherwise it will affect the neighbor establishment and route learning. Manually configure Router ID in the IPv4 address format in OSPFv3.

OSPFv3 supports multiple processes and uses the process number to identify a process. Different processes are independent of each other.

Table 42-2 Enable OSPFv3 Protocol

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Create an OSPFv3 process and enter the OSPF configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	Required Enable OSPFv3 process or enableOSPFv3 process from a VRF. By default, OSPFv3 protocol is disabled by the system. When OSPFv3 is enabled from the VRF, OSPFv3 process belonging to a VRF can only manage the interface belonging to that VRF
Configure the Router ID of OSPFv3 process	**router-id** *ipv4-address*	Required
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure an interface to enable the OSPFv3 protocol	**ipv6 router ospf** *process-id* **area** *area-id* [**instance-id** *instance-id*]	Required By default, the OSPFv3 protocol is disabled on the interface.

42.2.2 Configure OSPFv3 Area -E -A

To reduce the CPU and memory footprint of large amounts of database information, the OSPFv3 AS is divided into a number of areas. The areas are identified by a 32-bit area ID, which can be expressed as a decimal number in the range of 0 to 4294967295 or as an IP address in the range of 0.0.0.0 to 255.255.255.255. Area 0 or 0.0.0.0 represents OSPFv3 backbone area, and other non-0 areas are non-backbone areas. All the inter-area route information needs to be forwarded through the backbone area, and the non-backbone areas cannot exchange the route information directly.

Several types of routers are defined in OSPF v3:

- Internal Router: a device whose interfaces belong to an area;
- Area Border Router (ABR): a device connected to multiple areas;
- Automonous System Boundary Router (ASBR): a device that introduces external routes to OSPF v3 AS.

Configuration Conditions

Before configuring the OSPFv3 area, ensure that:

- The IPv6 forwarding function is enabled.
- Enable OSPFv3 protocol.

Configure OSPFv3 NSSA Area

Type-7 LSA instead of Type-5 LSA is allowed to be injected into Not-So-Stub-Area (NSSA). By configuring the Re-distribution, an external route is introduced to the NSSA and the ASBR of NSSA generates a Type-7 LSA and floods into that NSSA. The ABR of NSSA will convert Type-7 LSA to Type-5 LSAs and flood such Type-5 LSAs to the whole AS.

The OSPFv3 NSSA configured through the command **area** *area-id* **nssa no-summary** is called complete NSSA. OSPFv3 complete NSSA disables flooding of inter-area routes. At this point, ABR will generate a default route flooding into the NSSA. Devices in the NSSA will access the network outside the area through this default route.

Table 42-3 Configure OSPFv3 NSSA Area

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure NSSA area	**area** *area-id* **nssa** [**no-redistribution** / **no-summary** / **default-information-originate** [**metric** *metric-value* / **metric-type** *type-value*]]	Required By default, OSPFv3 area is not an NSSA area

NOTE

- The backbone area cannot be configured as an NSSA area.
- All devices in the same NSSA area must be configured as NSSA area, and devices with inconsistent area types cannot form adjacency relationships.

Configure OSPFv3 Stub Area

A Stub area does not allow AS external routes to flood to reduce the size of the link state database. When an area is configured as a Stub, ABR at the boundary of the Stub generates a default route and floods into the Stub area. Devices in the Stub area will access the network outside AS through this default route.

The OSPFv3 Stub area configured through the command **area** *area-id* **stub no-summary** is called complete Stub. OSPFv3 complete Stub area disables flooding of the inter-area routes and external routes. Devices in the area will access the networks outside the area and OSPFv3 AS through the default route.

Table 42-4 Configure OSPFv3 Stub area

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure Stub area	**area** *area-id* **stub** [**no-summary**]	Required By default, OSPFv3 area is not a Stub area

NOTE

- The backbone area cannot be configured as a Stub area.
- All devices in the same Stub area must be configured as Stub area, and devices with inconsistent area types cannot form adjacency relationships.

Configure an OSPFv3 Virtual Link

The non-backbone areas in OSPFv3 must synchronize databases and interact data through the backbone area. Therefore, it is required that all the non-backbone areas should be connected with the backbone area.

When this requirement is not met in some cases, a virtual link may be configured. After configuring the virtual link, you can configure the authentication method for the virtual link, modify the Hello interval, and so on. These parameters have the same meaning as the general OSPFv3 interface parameters.

Table 42-5 Configure an OSPFv3 Virtual Link

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure a virtual link	**area** *transit-area-id* **virtual-link** *neighbor-id* [**dead-interval** *seconds* / **hello-interval** *seconds* / **retransmit-interval** *seconds* / **transmit-delay** *seconds*]	Required By default, a virtual link will not be created

NOTE

- A virtual link must be configured between two ABRs.
- Two ABRs that configure the virtual link must in the same common area, also known as the Transit Area of virtual link.
- The Transit Area of virtual link cannot be Stub or NSSA.

42.2.3 Configure OSPFv3 Network Type *-E -A*

OSPFv3 divides the network into four types according to the type of link protocol:

- Broadcast Networks - When the link protocol is Ethernet or FDDI, OSPFv3 default network is broadcast;
- P2P (Point To Point Network) - When the link protocol is PPP, LAPB or HDLC, OSPFv3 default network is P2P;
- NBMA Network - When the link protocol is ATM, frame relay or X.25, OSPFv3 default network is NBMA;
- P2MP (Point To Multi-Point Network) - no link protocol is considered by OSPFv3 to be of type P2MP by default, and non-fully interconnected NBMA is typically configured as OSPFv3 P2MP.

The network type of the OSPFv3 interface can be modified as needed. The interface network type of OSPFv3 neighbors needs to be consistent, otherwise it will affect the normal learning of the route.

Configuration Conditions

Before configuring the OSPFv3 network type, ensure that:

- The IPv6 forwarding function is enabled.
- Enable OSPFv3 protocol.

Configure OSPFv3 Interface Network Type to Broadcast

Broadcast Networks supports multiple (two or more) devices that have the ability to interact with all devices on the network. OSPFv3 uses Hello packets to dynamically discover neighbors.

Table 42-6 Configure OSPFv3 Interface Network Type to Broadcast

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 interface network type to broadcast	**ipv6 ospf network broadcast**	Required By default, OSPFv3 interface network type is

Steps	Command	Description
		determined by the link layer protocol.

Configure OSPFv3 Interface Network Type to P2P

P2P is a network of two devices, each at one end of the point-to-point link. OSPFv3 uses Hello packets to dynamically discover neighbors.

Table 42-7 Configure OSPFv3 Interface Network Type to P2P

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 interface network type to P2P	**ipv6 ospf network point-to-point**	Required By default, OSPFv3 interface network type is determined by the link layer protocol.

Configure OSPFv3 Interface Network Type to NBMA

NBMA supports multiple (two or more) devices, but does not have the broadcast capability. The neighbors shall be specified manually.

Table 42-8 Configure OSPFv3 Interface Network Type to NBMA

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 interface network type to NBMA	**ipv6 ospf network non-broadcast**	Required By default, OSPFv3 interface network type is determined by the link layer protocol.
Configure an NBMA neighbor	**ipv6 ospf neighbor** *neighbor-ipv6-address* [**priority** *priority-value* /	Required

Steps	Command	Description
	poll-interval *interval-value* / **cost** *cost-value*] [**instance-id** *instance-id*]	In an NBMA, neighbors are manually specified

Configure OSPFv3 Interface Network Type to P2MP

When NBMA is not fully connected, the network type can be configured as P2MP to save network overhead. In a P2MP, neighbors are manually specified.

Table 42-9 Configure OSPFv3 Interface Network Type to P2MP

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 interface network type to P2MP	**ipv6 ospf network point-to-multipoint** [**non-broadcast**]	Required By default, OSPFv3 interface network type is determined by the link layer protocol.
Configure a P2MP neighbor	**ipv6 ospf neighbor** *neighbor-ipv6-address* [**priority** *priority-value* / **poll-interval** *interval-value* / **cost** *cost-value*] [**instance-id** *instance-id*]	Mandatory if the interface network type is configured as P2MP

42.2.4 Configure OSPFv3 Network Authentication *-E -A*

To prevent information leakage or hostile attacks on OSPFv3 devices, all packet interactions between OSPFv3 neighbors have encryption and authentication capability. The encryption and authentication type and algorithm may be NULL (no authentication), SHA1 authentication and MD5 authentication, which can be specified by the IPSec encryption and authentication policy.

After configuring the authentication, IPSec security features will encrypt and authenticate OSPFv3 protocol packet. Only after passing the decryption and authentication can the OSPFv3 receive the packet. Therefore, the authentication method, Spi ID, and IPSec encryption and authentication policy for the authentication key must be consistent with the OSPFv3 interface for establishing an adjacency relation. OSPFv3 authentication can be configured on the area and interface, with the priority of area authentication and interface authentication from low to high. That is, the interface authentication is used first, then the area authentication.

Configuration Conditions

Before configuring the OSPFv3 network authentication, ensure that:

- The IPv6 forwarding function is enabled.
- Enable OSPFv3 protocol.

Configure OSPFv3 Area Authentication

The area authentication configured in the OSPFv3 process area can make all interfaces in the area use the area authentication, and effectively avoid the repeated configuration of the same network authentication under the interface.

Table 42-10 Configure OSPFv3 Area Authentication

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure the area authentication method	**area** *area-id* **ipsec-tunnel** *tunnel-name*	Required By default, no area authentication is configured for OSPFv3.

Configure OSPFv3 Interface Authentication

When there are multiple OSPFv3 instances on an interface, you can specify an authentication method and key separately for a single instance. For an instance under the interface where the interface authentication is not specified, the authentication method under the area is used.

Table 42-11 Configure OSPFv3 Interface Authentication

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface authentication method	**ipv6 ospf ipsec-tunnel** *tunnel-name*{instance-id *instance-id*}	Required By default, no interface authentication method is configured for OSPFv3.

42.2.5 Configure OSPFv3 Route Generation -E -A

Configuration Conditions

Before configuring the OSPFv3 route generation, ensure that:

- The IPv6 forwarding function is enabled.
- Enable OSPFv3 protocol.

Configure OSPFv3 Route Re-distribution

When multiple routing protocols run on a single device and the routes from other protocols are introduced to OSPFv3 through Re-distribution. An OSPFv3 type 2 external route is generated by default with a metric value of 20. When introducing an external route by Re-distribution, you can modify the external route type, metric and Tag fields and associate with the specified route policy for route control and management.

Table 42-12 Configure OSPFv3 Route Re-distribution

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 route Re-distribution	**redistribute** *routing-protocol* [*protocol-id-or-name*] [**metric** *metric-value* / **metric-type** *type-value* / **tag** *tag-value* / **route-map** *map-name* / **match** *route-type*]	Required By default, OSPFv3 route Re-distribution is not configured.
Configure the metric value of an OSPFv3 external route	**default-metric** *metric-value*	Optional

NOTE

- When the **redistribute** *protocol* [*protocol-id*] **metric** and **default-metric** are configured simultaneously to set the metric value of the external route, the former has higher priority.

Configure OSPFv3 Default Route

After configuring the OSPFv3 Stub and the complete NSSA, a Type-3 default route is automatically generated. The NSSA does not automatically generate a default route. A Type-7 default route can be introduced to NSSA through the command **area** *area-id* **nssa default-information-originate**.

OSPFv3 cannot introduce a Type-5 default route through the **redistribute** command; if necessary, it can be done by configuring the **default-information forward [always]** command.

Table 42-13 Configure OSPFv3 Default Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 default route	**default-information originate** [**always** / **metric** *metric-value* / **metric-type** *metric-type* / **route-map** *route-map-name*]	Required By default, the external default route will not be introduced to OSPFv3 AS The introduced default route has the default metric 1 and the external type 2 **always** means that the default route is forced to be generated into the OSPFv3 AS, otherwise, it can be generated only a default route is available in the local routing table

42.2.6 Configure OSPFv3 Route Control *-E -A*

Configuration Conditions

Before configuring the OSPFv3 route control, ensure that:

- The IPv6 forwarding function is enabled.
- Enable OSPFv3 protocol.

Configure OSPFv3 Inter-area Route Summary

In OSPFv3, when ABR advertises other areas of the inter-area routes, each route is advertised separately as a Type-3 LSA. To reduce the size of the OSPFv3 database, you can use the inter-area route summary function to summarize a number of consecutive network segments in the area into a single route and only advertise the summarized routes.

Table 42-14 Configure OSPFv3 Inter-area Route Summary

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 inter-area route summary	**area** *area-id* **range** ipv6-*prefix/prefix-length* [**advertise** | **not-advertise**]	Required By default, ABR does not summarize the inter-area routes

NOTE

- The OSPFv3 inter-area route summary function only works on ABR.
- By default, the minimum cost value of the detailed routes is selected as the cost value of the route summary.

Configure OSPFv3 External Route Summary

When OSPFv3 Re-distributes external routes, each route is advertised separately in the external link state advertisements. To reduce the size of the OSPFv3 database, you can use the external route summary function to summarize a number of consecutive network segments outside AS into a single route and only advertise the summarized routes.

After configuring the command **summary-address** on ASBR, you can summarize Type-5 LSA and Type-7 LSA in the summary address range.

Table 42-15 Configure OSPFv3 External Route Summary

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 external route summary	**summary-prefix** *ipv6-prefix/prefix-length* [**not-advertise** | **tag** *tag-value*]	Required By default, ASBR does not summarize the external routes

NOTE

- The OSPFv3 external route summary function only works on ASBR.

Configure OSPFv3 Inter-area Route Filtration

ABR uses ACL or prefix-list for filtration in the in direction when receiving the inter-area routes and uses ACL or prefix-list for filtration in the out direction when advertising the inter-area routes.

Table 42-16 Configure OSPFv3 Inter-area Route Filtration

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 inter-area route filtration	**area** *area-id* **filter-list** { **access** { *access-list-name* | *access-list-number }* | **prefix** *prefix-list-name* } { **in** | **out** }	Required By default, ABR does not filter the inter-area routes

NOTE

- The OSPFv3 inter-area route filtration function only works on ABR.

Configure OSPFv3 External Route Filtration

Configure the external route filtration, i.e. use ACL or prefix-list to enable or disable flooding of routes outside the OSPFv3 AS into the OSPFv3 AS.

Table 42-17 Configure OSPFv3 External Route Filtration

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 external route filtration	**distribute-list** { **access** { *access-list-name* | *access-list-number }* | **prefix** *prefix-list-name* }	Required

Steps	Command	Description
	out [*routing-protocol* [*process-id*]]	By default, ASBR does not filter the external routes

NOTE

- The OSPFv3 external route filtration function only works on ASBR.

Configure OSPFv3 Route Installation Filtration

After OSPFv3 calculates the routes through LSA, the calculated OSPFv3 route information can be filtered to prevent some routes from being added to the routing table.

Table 42-18 Configure OSPFv3 Route Installation Filtration

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 route installation filtration	**distribute-list** { **access** { *access-list-name* | *access-list-number }* | **gateway** *prefix-list-name1* | **prefix** *prefix-list-name2* [**gateway** *prefix-list-name3*] | **route-map** *route-map-name*} **in** **[** *interface-name* **]**	Required By default, the OSPFv3 route installation filtration is not configured

NOTE

- The configured **prefix**, **gateway and route-map** filtrations are mutually exclusive with the configured ACL. For example, ACL filtration cannot be configured after configuration of the **prefix** filtration.
- The configured **route-map** and **prefix** filtrations are mutually exclusive with the configured **gateway** filtration.
- The configured **prefix** filtration overwrites the configured **gateway** filtration.

Configure the Cost Value of OSPFv3 Interface

By default, the OSPFv3 overhead is calculated by reference bandwidth/interface bandwidth.

Table 42-19 Configure the Cost Value of OSPFv3 Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the cost value of OSPFv3 interface	**ipv6 ospf cost** *cost* [**instance-id** *instance-id*]	Optional By default, it is calculated by reference bandwidth/interface bandwidth.

Configure OSPFv3 Reference Bandwidth

The interface reference bandwidth is mainly used to calculate the interface cost value, 100Mbit/s by default. The OSPFv3 interface cost is calculated by reference bandwidth/interface bandwidth. When the calculated result is greater than 1, the integer part is taken; if it's less than 1, it's 1. Therefore, in networks with bandwidth higher than 100Mbit/s, the optimal route will not be selected correctly. It can be solved by configuring an appropriate reference bandwidth with the **auto-cost reference-bandwidth** command.

Table 42-20 Configure OSPFv3 Reference Bandwidth

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 reference bandwidth	**auto-cost reference-bandwidth** *reference-bandwidth*	Optional By default, the reference bandwidth is 100Mbit/s

Configure the Administrative Distance of OSPFv3

The administrative distance is used to indicate the reliability of the routing protocol. After learning the routes to the same destination network from different routing protocols, the routes with a small administrative distance are selected with priority.

Table 42-21 Configure the Administrative Distance of OSPFv3

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure the administrative distance of OSPFv3	**distance [ospf** { **external** *distance* / **inter-area** *distance* / **intra-area** *distance* } | *distance*]	Optional By default, the administrative distance of OSPFv3 intra-area routes and inter-area routes is 110 and of external routes is 150

Configure the Maximum Number of OSPFv3 Load Balancing Entries

If there are multiple equivalent paths to the same destination address, load balancing is formed, which can improve the utilization rate of link and reduce the burden of link.

Table 42-22 Configure the Maximum Number of OSPFv3 Load Balancing Entries

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure the maximum number of OSPFv3 load balancing entries	**maximum-paths** *max-number*	Optional By default, the maximum number of OSPFv3 load balancing entries is 4

42.2.7 Configure OSPFv3 Network Optimization *-E -A*

Configuration Conditions

Before configuring OSPFv3 network optimization, ensure that:

- The IPv6 forwarding function is enabled.
- Enable OSPFv3 protocol.

Configure OSPFv3 Neighbor Keepalive Time

The OSPFv3 Hello packet is used to establish and keep alive the neighborship. The default send interval of the Hello packet is determined by the network type. The default send interval of Hello packet is 10s in the Broadcast Networks and P2P and is 30s in P2MP and NBMA.

The neighbor dead interval is used to judge the validity of the neighbor. The default is 4 times the Hello interval. If the OSPFv3 device does not receive the neighbor Hello message after the neighbor dead interval timeout, it believes that the neighbor has been invalid and actively deletes the neighbor.

Table 42-23 Configure OSPFv3 Neighbor Keepalive Time

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 Hello interval	**ipv6 ospf hello-interval** *interval-value* [**instance-id** *instance-id*]	Optional The default value, determined according to the network type, is 10s for the Broadcast Networks and P2P and 30s for P2MP and NBMA
Configure OSPFv3 neighbor dead interval	**ipv6 ospf dead-interval** *interval-value* [**instance-id** *instance-id*]	Optional The default is 4 times the Hello interval

NOTE

- The Hello interval and neighbor dead interval between neighbor OSPFv3 devices must be consistent, otherwise the neighborship cannot be established.
- When you modify the Hello interval, if the current neighbor dead interval is 4 times the Hello interval, the neighbor dead interval will also be automatically modified to maintain at 4 times; if the current neighbor dead interval is not 4 times the Hello interval, the neighbor dead interval remains unchanged.
- Modifying the dead interval does not affect the Hello interval.

Configure a Passive OSPFv3 Interface

Passive Interface is adopted in the dynamic routing protocol to effectively reduce the consumption of network bandwidth by the routing protocol. An OSPFv3 passive interface can be configured to advertise the route of the direct network segment where the interface is located through the interface enable command, but suppress the receiving and sending of OSPFv3 protocol packets on the interface.

Table 42-24 Configure a Passive OSPFv3 Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure a passive OSPFv3 interface	**passive-interface** {*interface-name*|**default**}	Required By default, no passive OSPF interface is configured

Configure OSPFv3 Demand Circuit

On P2P and P2MP links, to reduce the line cost, an OSPFv3 demand circuit can be configured to suppress the periodic sending of Hello packet and the periodic refresh of LSA packet. It is mainly used in charged link such as ISDN, SVC and X.25.

Table 42-25 Configure OSPFv3 Demand Circuit

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 demand circuit	**ipv6 ospf demand-circuit** [**instance-id** *instance-id*]	Required By default, the OSPFv3 demand circuit is disabled

Configure OSPFv3 interface priority

The interface priority is mainly used for the election of DR (Designated Router) and BDR (Backup Designated Router) in Broadcast Networks and NBMA, with the value range from 0 to 255. The higher the value, the higher the priority, 1 by default.

DR and BDR are elected by all devices in the same network segment according to interface priority and Router ID via Hello packet. The rules are as follows:

- The device with the highest priority is elected as DR and the device with the second highest priority is elected as BDR. Devices with the priority of 0 are not involved in election.
- If the interface priority is the same, the device with the highest Router ID is elected as DR, and the device with the second highest Router ID is elected as BDR.

When DR is invalidated, the BDR immediately becomes DR and a new BDR is elected.

Table 42-26 Configure OSPFv3 Interface Priority

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 interface priority	**ipv6 ospf priority** *priority-value* [**instance-id** *instance-id*]	Optional By default, the OSPFv3 interface priority is 1

NOTE

- Priorities only affect the election process. When DR and BDR have been elected in the network, the change of interface priority will not affect the election results, only the next DR or BDR election results; so DR is not necessarily the device with the highest interface priority, and BDR is not necessarily the device with the second highest interface priority.

Configure OSPFv3 OSPF Interface to Ignore MTU

When the neighbor devices of OSPFv3 interact the DD packet, they will check whether the MTU is the same by default. Otherwise, the adjacency relation cannot be formed. After OSPFv3 is configured to ignore the interface MTU check, the adjacency relation can be established even if the MTU is different.

Table 42-27 Configure OSPFv3 OSPF Interface to Ignore MTU

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 OSPF interface to ignore MTU	**ipv6 ospf mtu-ignore** [**instance-id** *instance-id*]	Required By default, MTU is performed Consistency check

Configure OSPFv3 Interface LSA Transmit Delay

The LSA transmit delay represents the time it takes for the LSA to flood to other devices, and the device sending the LSA will extend the interface transmit time to the aging time of the LSA to be sent. By default, the aging time increases by 1 when a flooded LSA passes through a device. The LSA transmit delay can be configured according to the network condition, with the value range of 1 ~ 840. It is generally used on low speed links.

Table 42-28 Configure OSPFv3 Interface LSA Transmit Delay

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 interface LSA transmit delay	**ipv6 ospf transmit-delay** *delay-value* **instance-id** [*instance-id*]	Optional By default, the interface LSA transmit delay is 1s.

Configure OSPFv3 LSA Retransmit

OSPFv3 adopts an acknowledgement mechanism to ensure the data interaction reliability. When an LSA floods on the device interface, the LSA will be added to the retransmit list of the neighbor. If an acknowledgment message is not received from the neighbor after the retransmit interval timeout, the LSA will be retransmitted until an acknowledgment message is received.

Table 42-29 Configure OSPFv3 LSA Retransmit

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 LSA retransmit interval	**ipv6 ospf retransmit-interval** *interval-value* [**instance-id** *instance-id*]	Optional By default, LSA retransmit interval is 5s.

Configure OSPFv3 SPF Computation Time

The route needs to be recomputed when the OSPFv3 network topology changes. When the network is constantly changing, frequent routing computation will occupy a lot of system resources. By adjusting the time parameter of SPF, the consumption of system resources caused by frequent changes of network is restrained.

Table 42-30 Configure OSPFv3 SPF Computation Time

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 SPF computation time	**timers throttle spf** *delay-time hold-time max-time*	Optional By default, *delay-time* is 5000ms, *hold-time* is 10000ms and *max-time* is 10000ms

NOTE

- The parameter *delay-time* represents the initial computation delay, *hold-time* represents the hold time, and *max-time* represents the maximum latency for two SPF computations. In the case of infrequent network changes, the interval of continuous routing computation is reduced to *delay-time*. In the case of frequent network changes, it can be adjusted accordingly and increased by *hold-time*×2^{n-2} (n is continuous routing computation times). The latency is extended according to the configured *hold-time* to a maximum of *max-time*.

42.2.8 Configure OSPFv3 GR *-E -A*

GR (Graceful Restart) is used to keep the route information at the forwarding level of the local device and neighbor device unchanged and the forwarding not affected during the master-backup switching; after the device switching and re-running, the two devices synchronize the route information at the protocol level and update the forward layer, so as to achieve the purpose of uninterrupted data forwarding during the switching process.

There are two roles in the GR process:

- GR Restarter end - a device that performs protocol GR.
- GR Helper end - a device that helps the protocol GR.

Distributed devices can serve as GR Restarter and GR Helper, while centralized devices can only serve as GR Helper to assist the Restarter end to complete GR.

Configuration Conditions

Before configuring OSPFv3 GR, ensure that:

- The IPv6 forwarding function is enabled.
- Enable OSPFv3 protocol.

Configure OSPFv3 GR Restarter

Table 42-31 Configure OSPFv3 GR Restarter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 GR	**nsf ietf**	Required By default, the GR function is disabled The function is enabled and the protocol shall support Opaque-LSA. By default, Opaque-LSA is supported.
Configure OSPFv3 GR period	**nsf interval** *grace-period*	Optional By default, the GR period is 95s

NOTE

- OSPFv3 GR is enabled only in the stack environment or dual master environment.

Configure OSPFv3 GR Helper

The GR Helper helps the Restarter complete GR. By default, the device enables the function and the command **nsf ietf helper disable** is used to disable GR Helper. The command **nsf ietf helper strict-lsa-checking** is used to configure the Helper to strictly check LSA in GR process. If checking any change in LSA, exit GR Helper mode.

Table 42-32 Configure OSPFv3 GR Helper

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPFv3 GR Helper	**nsf ietf helper** [**disable** | **strict-lsa-checking**]	Optional By default, the Helper is enabled and LSA will not be checked strictly

42.2.9 Configure OSPFv3 to Link with BFD *-E -A*

Configuration Conditions

Before configuring OSPFv3 to link with BFD, ensure that:

- The IPv6 forwarding function is enabled.
- Enable OSPFv3 protocol.

Configure OSPFv3 to Link with BFD

BFD provides a method for quickly detecting the state of the line between two devices. When BFD detection is enabled between two neighbor OSPFv3 devices, if there is a line fault between the devices, BFD will quickly detect the fault and notify OSPFv3 protocol, trigger OSPFv3 for routing computation and switch to the backup line to achieve quick route switching.

Table 42-33 Configure OSPFv3 to Link with BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure OSPFv3 specified interface to enable or disable BFD	**ipv6 ospf bfd [disable] [instance-id** *instance-id* **]**	Required By default, BFD function is disabled
Enter global configuration mode	**exit**	-
Enter the OSPFv3 configuration mode	**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure all interfaces of the OSPFv3 process to enable BFD	**bfd all-interfaces**	Optional

NOTE

- When BFD is configured in both OSPFv3 configuration mode and interface configuration mode, the priority of configuration under interface is higher.

42.2.10 OSPFv3 Monitoring and Maintaining *-E -A*

Table 42-34 OSPFv3 Monitoring and Maintaining

Command	Description
clear ipv6 ospf err-statistic	Clear OSPFv3 error statistics
clear ipv6 ospf [*process-id*] **process**	Reset the OSPFv3 process
clear ipv6 ospf [*process-id*] **redistribution**	Readvertise the external route
clear ipv6 ospf [*process-id*] **route**	Recompute the OSPFv3 route
clear ipv6 ospf statistics [*interface-name*]	Clear the OSPFv3 protocol statistics
show ipv6 ospf [*process-id*]	Show the basic information about OSPFv3
show ipv6 ospf [*process-id*] **border-routers**	Show the information on the router to the border device in OSPFv3
show ipv6 ospf core-info	Show the core information about OSPFv3 process
show ipv6 ospf [*process-id*] **database** [**database-summary** | **external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **nssa-external** | **grace** | **router** | **adv-router** *router-id* | **age** *lsa_age* | **max-age** | **self-originate**]	Show the information about the OSPFv3 database
show ipv6 ospf error-statistic	Show OSPFv3 error statistics
show ipv6 ospf event-list	Show OSPFv3 packet receive queue information
show ipv6 ospf interface [*interface-name* [**detail**]]	Show the OSPFv3 interface information
show ipv6 ospf [*process-id*] **neighbor** [*neighbor-id* | **all** | **detail** [**all**] | **interface** *interface-name* [**detail**] | **statistics**]	Show the information about the OSPFv3 neighbor

Command	Description
show ipv6 ospf [*process-id*] **route** [*ipv6-prefix*/*prefix-length* | **connected** | **external** | **inter-area** | **intra-area** | **statistic**]	Show OSPFv3 route information
show ipv6 ospf [*process-id*] **sham-links**	Show the information about the configured OSPFv3 sham link interface, including interface status, cost value and neighbor state
show ipv6 ospf [*process-id*] **topology area** [*area-id*]	Show the information about the OSPFv3 topology
show ipv6 ospf [*process- id*] **virtual-links**	Show the information about the OSPFv3 virtual link
show ipv6 ospf [**vrf** *vrf-name*]	Show all OSPFv3 process information and parameters in the specified vrf
show running-config ipv6 router ospf	Show the current running configuration of OSPFv3

42.3 OSPFv3 Typical Configuration Example

42.3.1 Configure Basic Functions of OSPFv3 ***-E -A***

Network Requirements

- All devices are configured with OSPFv3 protocol and are divided into Area 0, Area 1 and Area 2. Once configured, all devices can learn the route from each other.
- On back-to-back Ethernet interfaces, the OSPFv3 interface network type can be changed to point-to-point in order to accelerate OSPFv3 neighbor establishment. the interface network type of Area 2 is changed to point-to-point. Once configured, all devices can learn the route from each other.

Network Topology

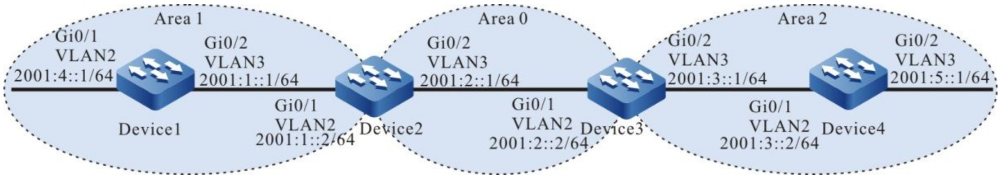


Figure 42-1 Networking for Configuring the Basic Functions of OSPFv3

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 addresses for the ports. (omitted)

Step 3: Configure OSPFv3 process and overwrite corresponding interfaces into different areas.

#Configure Device1, configure OSPFv3 process and overwrite the interface into area 1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 1
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 1
Device1(config-if-vlan3)#exit
```

#Configure Device2, configure OSPFv3 process and overwrite corresponding interfaces into areas 0 and 1.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 1
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#Configure Device3, configure OSPFv3 process and overwrite corresponding interfaces into areas 0 and 2.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 2
```

```
Device3(config-if-vlan3)#exit
```

#Configure Device4, configure OSPFv3 process and overwrite the interface into area 2.

```
Device4#configure terminal
Device4(config)#ipv6 router ospf 100
Device4(config-ospf6)#router-id 4.4.4.4
Device4(config-ospf6)#exit
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ipv6 router ospf 100 area 2
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan3
Device4(config-if-vlan3)#ipv6 router ospf 100 area 2
Device4(config-if-vlan3)#exit
```

NOTE

- In OSPFv3, the Router ID must be manually configured, and you must ensure that the Router ID for any two routers in AS is not the same.
- When the interface enables to OSPFv3, you need to specify which interface instance is enabled to the OSPFv3 process, and both instance numbers must be the same, default in instance 0.

#Query the OSPFv3 neighbor information and routing table of Device1.

```
Device1#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State          Dead Time   Interface                  Instance ID
2.2.2.2          1    Full/DR        00:00:38    vlan3              0

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 12:41:07 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:32:19 AM, vlan3
L   2001:1::1/128 [0/0]
    via ::, 12:32:18 AM, lo0
```

```
O   2001:2::/64 [110/2]
    via fe80::201:7aff:fe5e:6d45, 12:23:06 AM, vlan3
O   2001:3::/64 [110/3]
    via fe80::201:7aff:fe5e:6d45, 12:23:00 AM, vlan3
C   2001:4::/64 [0/0]
    via ::, 12:16:46 AM, vlan2
L   2001:4::1/128 [0/0]
    via ::, 12:16:45 AM, lo0
O   2001:5::/64 [110/4]
    via fe80::201:7aff:fe5e:6d45, 12:01:42 AM, vlan3
```

#Query the OSPFv3 neighbor and routing table of Device2.

```
Device2#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State          Dead Time   Interface                 Instance ID
1.1.1.1          1   Full/Backup     00:00:34    vlan2               0
3.3.3.3          1   Full/DR        12:00:33 AM    vlan3               0

Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
      U - Per-user Static route
      O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 12:50:36 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:43:05 AM, vlan2
L   2001:1::2/128 [0/0]
    via ::, 12:43:04 AM, lo0
C   2001:2::/64 [0/0]
    via ::, 12:40:01 AM, vlan3
L   2001:2::1/128 [0/0]
    via ::, 12:39:57 AM, lo0
O   2001:3::/64 [110/2]
    via fe80::2212:1ff:fe01:101, 12:34:00 AM, vlan3
O   2001:4::/64 [110/2]
    via fe80::201:7aff:fe61:7a24, 12:27:28 AM, vlan2
O   2001:5::/64 [110/3]
    via fe80::2212:1ff:fe01:101, 12:12:41 AM, vlan3
```

#Query OSPFv3 LSDB (link state database) of Device2.

```
Device2#show ipv6 ospf database


       OSPFv3 Router with ID (2.2.2.2) (Process 100)



         Link-LSA (Interface vlan2)
Link State ID   ADV Router      Age Seq#       CkSum  Prefix
0.0.0.1         1.1.1.1          81 0x80000001 0x8d18      1
0.0.0.1         2.2.2.2          78 0x80000001 0xf996      1



         Link-LSA (Interface vlan3)
Link State ID   ADV Router      Age Seq#       CkSum  Prefix
0.0.0.2         2.2.2.2          71 0x80000003 0x2467      1
0.0.0.1         3.3.3.3          35 0x80000003 0xcd12      1



         Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age Seq#       CkSum    Link
0.0.0.0         2.2.2.2          37 0x80000004 0x0dd6      1
0.0.0.0         3.3.3.3          25 0x80000007 0xda03      1



         Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age Seq#       CkSum
0.0.0.1         3.3.3.3          35 0x80000001 0x5790



         Inter-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age Seq#       CkSum  Prefix
0.0.0.2         2.2.2.2          42 0x80000007 0x9e25 2001:1::/64
0.0.0.3         2.2.2.2          23 0x80000002 0xcef4 2001:4::/64
0.0.0.1         3.3.3.3          35 0x80000005 0xaa16 2001:3::/64
0.0.0.3         3.3.3.3          55 0x80000001 0xc0fe 2001:5::/64



         Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age Seq#       CkSum  Prefix  Reference
0.0.0.3         3.3.3.3          34 0x80000001 0xb2d3      1  Network-LSA
```

```
               Router-LSA (Area 0.0.0.1)
Link State ID   ADV Router      Age Seq#       CkSum    Link
0.0.0.0         1.1.1.1          41 0x80000004 0xc726     1
0.0.0.0         2.2.2.2          37 0x80000004 0xac3c     1


               Network-LSA (Area 0.0.0.1)
Link State ID   ADV Router      Age Seq#       CkSum
0.0.0.1         2.2.2.2          42 0x80000001 0x21d2


               Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router      Age Seq#       CkSum  Prefix
0.0.0.1         2.2.2.2          42 0x80000004 0xbc0a 2001:2::/64
0.0.0.4         2.2.2.2          19 0x80000001 0xb80c 2001:3::/64
0.0.0.5         2.2.2.2          19 0x80000001 0xd0ef 2001:5::/64


               Intra-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router      Age Seq#       CkSum  Prefix  Reference
0.0.0.1         1.1.1.1          35 0x80000005 0xc4ce     1  Router-LSA
0.0.0.3         2.2.2.2          41 0x80000001 0x8807     1  Network-LSA
```

For Device2, 2001:3::/642 and 2001:5::/64 are inter-area routes. The LSA information of relevant routes can be queried from Inter-Area-Prefix-LSA (Area 0.0.0.0) and of intra-area routes may be queried only by show ipv6 ospf database intra-prefix.

Step 4: Configure OSPFv3 interface network type to P2P.

#Configure Device3 and change OSPFv3 network type of the interface vlan3 to P2P.

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 ospf network point-to-point
Device3(config-if-vlan3)#exit
```

#Configure Device4 and change OSPFv3 network type of the interface vlan2 to P2P.

```
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ipv6 ospf network point-to-point
Device4(config-if-vlan2)#exit
```

Step 5: Check the result.

#Query the OSPFv3 neighbor and routing table of Device3.

```
Device3#show ipv6 ospf neighbor
```

```
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface                    Instance ID
2.2.2.2          1   Full/Backup     00:00:39    vlan2           0
4.4.4.4          1   Full/ -         00:00:39    vlan3           0

Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
     via ::, 1d:9:10:10 AM, lo0
O   2001:1::/64 [110/2]
     via fe80::201:7aff:fe5e:6d46, 2:07:25 AM, vlan2
C   2001:2::/64 [0/0]
     via ::, 3:07:51 AM, vlan2
L   2001:2::2/128 [0/0]
     via ::, 3:07:48 AM, lo0
C   2001:3::/64 [0/0]
     via ::, 3:07:41 AM, vlan3
L   2001:3::1/128 [0/0]
     via ::, 3:07:39 AM, lo0
O   2001:4::/64 [110/3]
     via fe80::201:7aff:fe5e:6d46, 2:07:25 AM, vlan2
O   2001:5::/64 [110/2]
     via fe80::201:2ff:fe03:405, 12:00:22 AM, vlan3
```

NOTE

- DR and BDR will not be elected when a P2P establishes OSPFv3 adjacency.

#Query the OSPFv3 neighbor and routing table of Device4.

```
Device4#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface                    Instance ID
3.3.3.3          1   Full/ -         00:00:38    vlan2              0

Device4#show ipv6 route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
    via ::, 12:05:34 AM, lo0
O   2001:1::/64 [110/3]
    via fe80::2212:1ff:fe01:102, 12:03:12 AM, vlan2
O   2001:2::/64 [110/2]
    via fe80::2212:1ff:fe01:102, 12:03:12 AM, vlan2
C   2001:3::/64 [0/0]
    via ::, 12:04:34 AM, vlan2
L   2001:3::2/128 [0/0]
    via ::, 12:04:31 AM, lo0
O   2001:4::/64 [110/4]
    via fe80::2212:1ff:fe01:102, 12:03:12 AM, vlan2
C   2001:5::/64 [0/0]
    via ::, 12:03:14 AM, vlan3
L   2001:5::1/128 [0/0]
    via ::, 12:03:13 AM, lo0
```

As you can see, after modifying the OSPFv3 interface network type to P2P, a neighbor can be established normally and can learn the route normally.

42.3.2 Configure OSPFv3 to Use IPSec Encryption and Authentication *-E -A*

Network Requirements

- All routers run OSPFv3 and the whole AS is divided into 2 areas.
- Device1, Device2 and Device3 uses the IPSec tunnel to encrypt and authenticate the OSPFv3 protocol packets. Device1 and Device2 use ESP transport encapsulation mode, with the encryption algorithm of 3des and authentication algorithm of sha1. Device2 and Device3 use ESP transport encapsulation mode, with the encryption algorithm of aes128 and ESP authentication algorithm of sm3.
- After configuration, the devices can establish a neighbor normally and learn the routes from each other.

Network Topology

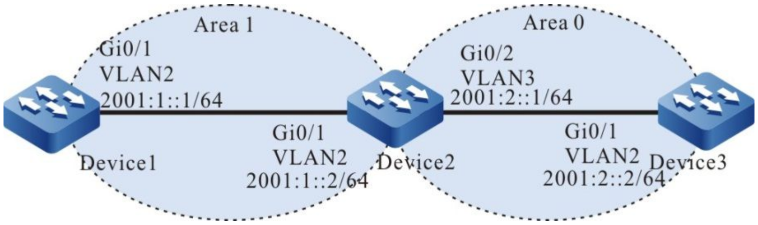


Figure 42-2 Networking for Configuring OSPFv3 to Use IPSec Encryption and Authentication

Configuration Steps

Step 1: Configure IPv6 addresses for the ports. (omitted)

Step 2: Configure the OSPFv3 process and enable OSPFv3 at the corresponding interfaces.

#Configure the OSPFv3 process of Device1, Device2 and Device3 and enable OSPFv3 at the interface.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 1
Device1(config-if-vlan2)#exit

Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 1
Device2(config-if- vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if- vlan3)#ipv6 router ospf 100 area 0
Device2(config-if- vlan3)#exit

Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
```

Step 3: Configure IPSec proposal and manual tunnel.

#Configure Device1, create an IPSec proposal a, use ESP transport encapsulation mode, with the encryption algorithm of 3des and authentication algorithm of sha1, create an IPSec manual tunnel a and configure the SPI and key.

```
Device1(config)#crypto ipsec proposal a
Device1(config-ipsec-prop)#mode transport
Device1(config-ipsec-prop)#esp 3des sha1
Device1(config-ipsec-prop)#exit
Device1(config)#crypto tunnel a manual
Device1(config-manual-tunnel)#set ipsec proposal a
Device1(config-manual-tunnel)#set inbound esp 1000 encryption 0 111111111111111111111111 authentication 0 aaaaaaaa
aaaaaaaaaaaa
Device1(config-manual-tunnel)#set outbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaaaa authentication 0 11111111
111111111111
Device1(config-manual-tunnel)#exit
```

#Configure Device2, create an IPSec proposal a, use ESP transport encapsulation mode, with the encryption algorithm of 3des and authentication algorithm of sha1, create an IPSec manual tunnel a and configure the SPI and key; create an IPSec proposal b, use ESP transport encapsulation mode, with the encryption algorithm of aes128 and authentication algorithm of sm3, create an IPSec manual tunnel b and configure the SPI and key.

```
Device2(config)#crypto ipsec proposal a
Device2(config-ipsec-prop)#mode transport
Device2(config-ipsec-prop)#esp 3des sha1
Device2(config-ipsec-prop)#exit
Device2(config)#crypto tunnel a manual
Device2(config-manual-tunnel)#set ipsec proposal a
Device2(config-manual-tunnel)#set inbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaaaa authentication 0 111111111
11111111111
Device2(config-manual-tunnel)#set outbound esp 1000 encryption 0 111111111111111111111111 authentication 0 aaaaaaaa
aaaaaaaaaaaa
Device2(config-manual-tunnel)#exit
Device2(config)#crypto ipsec proposal b
Device2(config-ipsec-prop)#mode transport
Device2(config-ipsec-prop)#esp aes128 sm3
Device2(config-ipsec-prop)#exit
Device2(config)#crypto tunnel b manual
Device2(config-manual-tunnel)#set ipsec proposal b
Device2(config-manual-tunnel)#set inbound esp 2001 encryption 0 1111111111111111 authentication 0 aaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaa
Device2(config-manual-tunnel)#set outbound esp 2000 encryption 0 1111111111111111 authentication 0 1111111111111111
1111111111111111
Device2(config-manual-tunnel)#exit
```

#Configure Device3, create an IPSec proposal b, use ESP transport encapsulation mode, with the encryption algorithm of aes128 and authentication algorithm of sm3, create an IPSec manual tunnel b and configure the SPI and key.

```
Device3(config)#crypto ipsec proposal b
Device3(config-ipsec-prop)#mode transport
Device3(config-ipsec-prop)#esp aes128 sm3
Device3(config-ipsec-prop)#exit
Device3(config)#crypto tunnel b manual
Device3(config-manual-tunnel)#set ipsec proposal b
Device3(config-manual-tunnel)#set inbound esp 2000 encryption 0 1111111111111111 authentication 0 11111111111111111
111111111111111
Device3(config-manual-tunnel)#set outbound esp 2001 encryption 0 1111111111111111 authentication 0 aaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaa
Device3(config-manual-tunnel)#exit
```

Step 4: Bind the corresponding IPSec tunnels of the areas in the OSPFv3 process.

#In OSPFv3 process of Device1, bind area 1 to IPSec tunnel a.

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#area 1 ipsec-tunnel a
Device1(config-ospf6)#exit
```

#In OSPFv3 process of Device2, bind area 1 to IPSec tunnel a and area 0 to IPSec tunnel b.

```
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#area 1 ipsec-tunnel a
Device2(config-ospf6)#area 0 ipsec-tunnel b
Device1(config-ospf6)#exit
```

#In OSPFv3 process of Device3, bind area 0 to IPSec tunnel b.

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#area 0 ipsec-tunnel b
Device3(config-ospf6)#exit
```

Step 5: Check the result.

#Query the OSPFv3 process information of Device1.

```
Device1#show ipv6 ospf 100
  Routing Process "OSPFv3 (100)" with ID 1.1.1.1
 Process bound to VRF default
 IETF graceful-restarter support disabled
 IETF gr helper support enabled
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 5
 Number of LSA received 5
 Number of areas in this router is 1
 Not Support Demand Circuit lsa number is 0
 Autonomy system support flood DoNotAge Lsa
    Area 0.0.0.1
        Number of interfaces in this area is 1
        IPSec Tunnel Name:a , ID: 154
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent sham-link neighbors in this area is 0
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 4 times
        LSA walker due in 00:00:02
        Number of LSA 4.  Checksum Sum 0x2FC53
        Number of Unknown LSA 0
        Not Support Demand Circuit lsa number is 0
        Indication lsa (by other routers) number is: 0,
        area support flood DoNotAge Lsa
```

As you can see, the area is bound to IPSec tunnel a, with ID of a random value between 0 and 1023.

#Query the IPSec tunnel information of Device1.

```
Device1#show crypto tunnel a
get the manual tunnel
Crypto tunnel a : MANUAL
        policy name : (null)
        peer address :
        local interface : (null) address :
        Ipsec proposal : a
        Inbound :
          esp : spi: 1000 encription key: ******** authentication key: ********
          ah spi: 0 authentication key: (null)
        Outbound :
          esp spi: 1001 encryption key: ******** authentication key: ********
          ah spi: 0 authentication key: (null)
        route ref : 1
        route asyn : 1
        route rt_id : 154
```

As you can see, route rt_id is equal to ID in show ipv6 ospf 100.

#Query the information about IPSec tunnel encryption type of Device1.

```
Device1#show crypto ipsec sa tunnel a
route policy:
  the pairs of ESP ipsec sa : id :0 , algorithm : 3DES HMAC-SHA1-96
    inbound esp ipsec sa :  spi : 0x3e8(1000)  crypto m_context(s_context) : 0x4cd3ba78 / 0x4cd3bae0
        current input 26 packets, 2 kbytes
        encapsulation mode : Transport
        replay protection : OFF
        remaining lifetime (seconds/kbytes) : 0/0
        uptime is 0 hour 4 minute 45 second
    outbound esp ipsec sa :  spi : 0x3e9(1001)  crypto m_context(s_context) : 0x4cd3bb48 / 0x4cd3bbb0
    current output 39 packets, 3 kbytes
    encapsulation mode : Transport
    replay protection : OFF
    remaining lifetime (seconds/kbytes) : 0/0
    uptime is 0 hour 4 minute 45 second

total sa and sa group is 1
```

As you can see, IPSec tunnel a uses ESP transport encapsulation mode, with the encryption algorithm of 3des and authentication algorithm of sha1.

```
#Query the OSPFv3 interface information of Device1.
Device1#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
  Interface ID 50331913
  IPv6 Prefixes
    fe80::201:7aff:fecf:fbec/10 (Link-Local Address)
    2001 :1::1/64
  Interface ID 13
  OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:41:10, MTU 1500
    Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
    IPSec tunnel(Area):a, ID:154
    Transmit Delay is 1 sec, State Backup, 3 state change, Priority 1
    Designated Router (ID) 2.2.2.2
      Interface Address fe80::200:1ff:fe7a:adf0
    Backup Designated Router (ID) 1.1.1.1
      Interface Address fe80::201:7aff:fecf:fbec
    Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
      Hello due in 12:00:06 AM
    Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 2 sent 3, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 3 sent 2, Discarded 0
```

As you can see, the interface is bound to IPSec tunnel a, with ID of a random value between 0 and 1023.

#Query the OSPFv3 neighbor information and core routing table of Device1.

```
Device1#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID    Pri    State       Dead Time      Interface              Instance ID
2.2.2.2        1      Full/DR     00:00:39       vlan2     0

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
     via ::, 4d:4:06:36 AM, lo0
C   2001:1::/64 [0/0]
     via ::, 3:00:53 AM, vlan2
L   2001:1::1/128 [0/0]
     via ::, 3:00:49 AM, lo0
O   2001:2::/64 [110/2]
     via fe80::201:7aff:fec9:1cdd, 2d:00:03:49, vlan2
```

On Device1, the neighbor is normally established and the route is learnt normally.

#Query the OSPFv3 interface information of Device3.

```
Device3#show ipv6 ospf 100
 Routing Process "OSPFv3 (100)" with ID 3.3.3.3
 Process bound to VRF default
 IETF graceful-restarter support disabled
 IETF gr helper support enabled
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 5
 Number of LSA received 6
 Number of areas in this router is 1
 Not Support Demand Circuit lsa number is 0
 Autonomy system support flood DoNotAge Lsa
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        IPSec Tunnel Name:b , ID: 2
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent sham-link neighbors in this area is 0
        SPF algorithm executed 4 times
        LSA walker due in 00:00:02
        Number of LSA 4.  Checksum Sum 0x24272
        Number of Unknown LSA 0
        Not Support Demand Circuit lsa number is 0
        Indication lsa (by other routers) number is: 0,
        area support flood DoNotAge Lsa
```

As you can see, the area is bound to IPSec tunnel b, with ID of a random value between 0 and 1023.

#Query the IPSec tunnel information of Device3.

```
Device3#show crypto tunnel b
get the manual tunnel
Crypto tunnel b : MANUAL
        policy name : (null)
        peer address :
        local interface : (null) address :
        Ipsec proposal : b
        Inbound :
          esp : spi: 2000 encription key: ******** authentication key: ********
          ah spi: 0 authentication key: (null)
        Outbound :
          esp spi: 2001 encryption key: ******** authentication key: ********
          ah spi: 0 authentication key: (null)
        route ref : 1
        route asyn : 1
        route rt_id : 2
```

As you can see, route rt_id is equal to ID in show ipv6 ospf 100.

#Query the information about IPSec tunnel encryption type of Device3.

```
Device3#show crypto ipsec sa tunnel b
route policy:
  the pairs of ESP ipsec sa : id : 0, algorithm : AES128 HMAC-SM3
       inbound esp ipsec sa :  spi : 0x7d0(2000)  crypto m_context(s_context) : 0x6a0d9a98 /
       0x6a0d9a30
        current input 53 packets, 5 kbytes
        encapsulation mode : Transport
        replay protection : OFF
        remaining lifetime (seconds/kbytes) : 0/0
        uptime is 0 hour 6 minute 40 second
       outbound esp ipsec sa :  spi : 0x7d1(2001)  crypto m_context(s_context) : 0x6a0d99c8 /
       0x6a0d9960
        current output 52 packets, 5 kbytes
        encapsulation mode : Transport
        replay protection : OFF
        remaining lifetime (seconds/kbytes) : 0/0
        uptime is 0 hour 6 minute 40 second

total sa and sa group is 1
```

As you can see, IPSec tunnel uses ESP transport encapsulation mode, with the encryption algorithm of aes128 and authentication algorithm of sm3.

#Query the OSPFv3 interface information of Device3.

```
Device3#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
  Interface ID 50331899
  IPv6 Prefixes
    fe80::200:1ff:fe7a:adf0/10 (Link-Local Address)
    2001 :2::1/64
  Interface ID 9
  OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 12:50:39 AM, MTU 1500
    Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
    IPSec tunnel(Area):b, ID:2
    Transmit Delay is 1 sec, State DR, 4 state change, Priority 1
    Designated Router (ID) 2.2.2.2
      Interface Address fe80::200:1ff:fe7a:adf0
    Backup Designated Router (ID) 1.1.1.1
      Interface Address fe80::201:7aff:fecf:fbec
    Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
      Hello due in 12:00:02 AM
    Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 272 sent 316, DD received 12 sent 9
  LS-Req received 3 sent 5, LS-Upd received 19 sent 18
  LS-Ack received 11 sent 13, Discarded 0
```

As you can see, the interface is bound to IPSec tunnel b, with ID of a random value between 0 and 1023.

#Query the OSPFv3 neighbor information and core routing table Device3.

```
Device3#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID    Pri     State         Dead Time       Interface            Instance ID
2.2.2.2        1       Full/Backup   00:00:35        vlan2  0

Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M – Management


L   ::1/128 [0/0]
     via ::, 9:53:53 AM, lo0
O   2001:1::/64 [110/2]
     via fe80::ae9c:e4ff:fe77:889e, 00:23:36, vlan2
C   2001:2::/64 [0/0]
     via ::, 3:05:16 AM, vlan2
L   2001:2::2/128 [0/0]
     via ::, 3:05:13 AM, lo0
```

On Device3, the neighbor is normally established and the route is learnt normally.

Step 6: Bind the corresponding IPSec tunnels at the OSPFv3 interface.

#Configure Device1 and bind the interface vlan2 to IPSec tunnel a.

```
Device1(config)#interface vlan2
Device1(config-if- vlan2)#ipv6 ospf ipsec-tunnel a
Device1(config-if- vlan2)#exit
```

#Configure Device2 and bind the interface vlan2 to IPSec tunnel a; bind the interface vlan3 to IPSec tunnel b.

```
Device2(config)#interface vlan2
Device2(config-if- vlan2)#ipv6 ospf ipsec-tunnel a
Device2(config-if- vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 ospf ipsec-tunnel b
Device2(config-if-vlan3)#exit
```

#Configure Device3 and bind the interface vlan2 to IPSec tunnel b.

```
Device3(config)#interface vlan2
                              Device3(config-if- vlan2)#ipv6 ospf ipsec-tunnel b
Device3(config-if- vlan2)#exit
```

Step 7: Check the result.

#Query the OSPFv3 interface information of Device1.

```
Device1#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
  Interface ID 50331913
  IPv6 Prefixes
    fe80::201:7aff:fecf:fbec/10 (Link-Local Address)
    2001 :1::1/64
  Interface ID 13
  OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:41:10, MTU 1500
    Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
    IPSec tunnel:a, ID:154
    Transmit Delay is 1 sec, State Backup, 3 state change, Priority 1
    Designated Router (ID) 2.2.2.2
      Interface Address fe80::200:1ff:fe7a:adf0
    Backup Designated Router (ID) 1.1.1.1
      Interface Address fe80::201:7aff:fecf:fbec
    Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
      Hello due in 12:00:06 AM
    Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 2 sent 3, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 3 sent 2, Discarded 0
```

As you can see, the interface is bound to IPSec tunnel a, with ID of a random value between 0 and 1023.

#Query the OSPFv3 Core routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
     via ::, 4d:4:06:36 AM, lo0
C   2001:1::/64 [0/0]
     via ::, 3:00:53 AM, vlan2
L   2001:1::1/128 [0/0]
     via ::, 3:00:49 AM, lo0
O   2001:2::/64 [110/2]
     via fe80::201:7aff:fec9:1cdd, 2d:00:03:49, vlan2
```

On Device1, the route is learnt normally.

#Query the OSPFv3 interface information of Device3.

```
Device3#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
  Interface ID 50331899
  IPv6 Prefixes
    fe80::200:1ff:fe7a:adf0/10 (Link-Local Address)
    2001 :2::1/64
  Interface ID 9
  OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 12:50:39 AM, MTU 1500
    Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
    IPSec tunnel:b, ID:2
    Transmit Delay is 1 sec, State DR, 4 state change, Priority 1
    Designated Router (ID) 2.2.2.2
      Interface Address fe80::200:1ff:fe7a:adf0
    Backup Designated Router (ID) 1.1.1.1
      Interface Address fe80::201:7aff:fecf:fbec
    Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
```

```
     Hello due in 12:00:02 AM
   Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 272 sent 316, DD received 12 sent 9
  LS-Req received 3 sent 5, LS-Upd received 19 sent 18
  LS-Ack received 11 sent 13, Discarded 0
```

As you can see, the interface is bound to IPSec tunnel b, with ID of a random value between 0 and 1023.

#Query the OSPFv3 core routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M – Management


L   ::1/128 [0/0]
     via ::, 9:53:53 AM, lo0
O   2001:1::/64 [110/2]
     via fe80::ae9c:e4ff:fe77:889e, 00:23:36, vlan2
C   2001:2::/64 [0/0]
     via ::, 3:05:16 AM, vlan2
L   2001:2::2/128 [0/0]
     via ::, 3:05:13 AM, lo0
```

On Device3, the route is learnt normally.

NOTE

- When configuringOSPFv3 to bind IPSec tunnel, you can configure only area binding or interface binding, or both.
- When the area binding and interface binding are configured with IPSec tunnel, the interface binding takes precedence.

42.3.3 Configure OSPFv3 to Link with BFD *-E -A*

Network Requirements

- All devices are configured with OSPFv3 protocol.
- The line between Device1 and Device3 enables BFD detection function. When a fault occurs in the line, BFD will quickly detect the fault and inform OSPFv3. OSPFv3 switches the route to Device2 for communication.

Network Topology

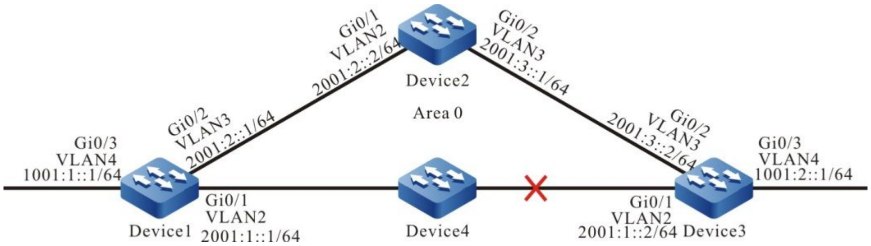


Figure 42-3 Networking for Configuring OSPFv3 to Link with BFD

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 addresses for the ports. (omitted)

Step 3: Configure the OSPFv3 process.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 router ospf 100 area 0
Device1(config-if-vlan4)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
```

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)#exit
```

Step 4: Configure OSPFv3 to link with BFD.

#Configure Device1.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 ospf bfd
Device1(config-if-vlan2)#exit
```

#Configure Device3.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 ospf bfd
Device3(config-if-vlan2)#exit
```

Step 5: Check the result.

#Query the OSPFv3 neighbor information and routing table of Device1.

```
Device1#show ipv6 ospf neighbor 3.3.3.3
OSPFv3 Process (100)

 Neighbor 3.3.3.3,interface address fe80::2212:1ff:fe01:104
   In the area 0.0.0.0 via interface vlan4, BFD enabled
   DR is 3.3.3.3 BDR is 1.1.1.1
   Neighbor priority is 1, State is Full, 6 state changes
   Options is 0x13 (-|R|-|-|E|V6)
   Dead timer due in 12:00:37 AM
   Neighbor is up for 12:01:31 AM
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
   Thread Inactivity Timer on
   Thread Database Description Retransmission off, 0 times
   Thread Link State Request Retransmission off, 0 times
   Thread Link State Update Retransmission off, 0 times

Device1#show ipv6 route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
     via ::, 1:15:27 AM, lo0
C   1001:1::/64 [0/0]
     via ::, 1:15:27 AM, vlan4
L   1001:1::1/128 [0/0]
     via ::, 1:15:27 AM, lo0
O   1001:2::/64 [110/2]
     via fe80::2212:1ff:fe01:104, 12:02:40 AM, vlan2
C   2001:1::/64 [0/0]
     via ::, 1:15:27 AM, vlan2
L   2001:1::1/128 [0/0]
     via ::, 1:15:27 AM, lo0
C   2001:2::/64 [0/0]
     via ::, 1:15:27 AM, vlan3
L   2001:2::1/128 [0/0]
     via ::, 1:15:27 AM, lo0
O   2001:3::/64 [110/2]
     via fe80::201:7aff:fe5e:6d45, 12:02:40 AM, vlan3
                [110/2]
     via fe80::2212:1ff:fe01:104, 12:02:40 AM, vlan2
```

It can be seen from the OSPFv3 neighbor information that BFD has been enabled and the route 1001:2::/64 prefers the line between Device1 and Device3 for communication.

#Query the BFD session of Device1.

```
Device1#show bfd session ipv6 detail
Total ipv6 session number: 1
OurAddr                        NeighAddr                       State      Holddown    Interface
fe80::201:7aff:fe61:7a25             fe80::2212:1ff:fe01:104              UP         5000        vlan2
Type:ipv6 direct
Local State:UP  Remote State:UP  Up for: 0h:0m:4s  Number of times UP:1
Local Discriminator:5  Remote Discriminator:95
Send Interval:1000ms  Detection time:5000ms(1000ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:1000  MinRxInt:1000  Multiplier:5
Remote MinTxInt:1000  Remote MinRxInt:1000  Remote Multiplier:5
Registered protocols:OSPFv3
```

It can be seen that OSPFv3 coordinates with BFD successfully and the session is established normally.

#After a fault occurs in the line between Device1 and Device3, BFD will quickly detect the fault and inform OSPFv3. OSPFv3 switches the route to Device2 for communication. Query the routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
   via ::, 1:16:10 AM, lo0
C   1001:1::/64 [0/0]
   via ::, 1:16:10 AM, vlan4
L   1001:1::1/128 [0/0]
   via ::, 1:16:10 AM, lo0
O   1001:2::/64 [110/3]
   via fe80::201:7aff:fe5e:6d45, 12:00:07 AM, vlan3
C   2001:1::/64 [0/0]
   via ::, 1:16:10 AM, vlan2
L   2001:1::1/128 [0/0]
   via ::, 1:16:10 AM, lo0
C   2001:2::/64 [0/0]
   via ::, 1:16:10 AM, vlan3
L   2001:2::1/128 [0/0]
   via ::, 1:16:10 AM, lo0
O   2001:3::/64 [110/2]
   via fe80::201:7aff:fe5e:6d45, 12:03:22 AM, vlan3
```

Device3 behaves similarly to Device1.

43 IS-IS

43.1 Overview

IS-IS (Intermediate System to Intermediate System) is an Interior Gateway Protocol (IGP) based on SPF algorithm. The basic design idea of IS-IS is consistent with the algorithm and OSPF. IS-IS is a routing protocol based on the link layer, independent of the network layers (IPv4, IPv6, OSI) and not constrained by the network layers, so it has good scalability.

IS-IS can support the routing of multiple protocol stacks simultaneously, including IPv4, IPv6, and OSI. IS-IS was originally used in the OSI protocol stack (ISO10589) and then extended for routing in the IPv4 protocol stack (RFC1195) and IPv6 protocol stack (RFC5308). After extension, it can support the CSPF computation of MPLS-TE (RFC3784).

The IS-IS protocol has the advantages of good compatibility (well compatible with different devices that achieve different extensions), large network capacity, support for multiple protocol stacks at the same time, smooth upgrade and simple compared with OSPF. Thus, IS-IS is suitable for large core backbone networks. This section describes how to configure the IS-IS dynamic routing protocol on a Device for network interconnection.

43.2 IS-IS Function Configuration

Table 43-1 IS-IS Function List

Configuration task	
Configure basic functions of IS-IS	Enable IS-IS protocol
	Configure IS-IS VRF properties
Configure IS-IS level attributes	Configure IS-IS level attributes
Configure IS-IS route generation	Configure IS-IS default route
	Configure IS-IS route Re-distribution
Configure IS-IS route control	Configure IS-IS metric style
	Configure IS-IS interface metric value
	Configure the administrative distance of IS-IS
	Configure IS-IS route summary

Configuration task	
	Configure the maximum number of IS-IS load balancing entries
	Configure IS-IS inter-level route leakage
	Configure IS-IS ATT bit
Configure IS-IS network optimization	Configure IS-IS interface priority
	Configure a passive IS-IS interface
	Configure IS-IS Hello packet parameters
	Configure IS-IS LSP packet parameters
	Configure IS-IS SNP packet parameters
	Configure IS-IS SPF computing interval
	Configure IS-IS maximum area number
	Configure IS-IS hostname mapping
	Configure IS-IS interface to join Mesh group
Configure IS-IS network authentication	Configure IS-IS neighbor authentication
	Configure IS-IS route authentication
Configure IS-IS to link with BFD	Configure IS-IS to link with BFD
Configure IS-IS GR	Configure IS-IS GR

43.2.1 Configure Basic Functions of IS-IS *-E -A*

Configuration Conditions

Before using the IS-IS protocol, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.

The network layer address of the interface is configured to make the adjacent node network layers accessible;

Enable IS-IS Protocol

Multiple IS-IS processes can run in the system at the same time, and are distinguished by different process names.

Table 43-2 Enable IS-IS Protocol

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create an IS-IS process and enter the IS-IS configuration mode	**router isis** [*area-tag*]	Required By default, no IS-IS process runs in the system and *area-tag* is the process name.
Configure a network entity title for IS-IS	**net** *entry-title*	Required By default, IS-IS has no network entity title
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable IS-IS at the interface	**ip router isis** [*area-tag*]	Required By default, IS-IS is not enabled at the interface

NOTE

- IS-IS cannot run without a network entity title.

Configure IS-IS VRF Properties

There may be multiple IS-IS processes in the same VRF, but only one Level-2 IS-IS process.

Table 43-3 Configure IS-IS VRF Properties

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-

Steps	Command	Description
Configure IS-IS VRF properties	**vrf** *vrf-name*	Optional By default, IS-IS process is in the global VRF

43.2.2 Configure IS-IS Level Attributes *-E -A*

Configuration Conditions

Before configuring IS-IS level attributes, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible.
- Enable IS-IS protocol.

Configure IS-IS Level Attributes

IS-IS level attributes are divided into global level attributes and interface level attributes; the global level attributes are of IS-IS intermediate system category, divided into the following three types:

- Level-1 intermediate system: only Level-1 link state database can advertise and learn the routes of Level-1 area;
- Level-2 intermediate system: only Level-2 link state database can advertise and learn the routes of Level-2 area;
- Level-1-2 intermediate system: the link state database with both Level-1 and Level-2 can advertise and learn the routes of Level-1 and Level-2. It is the interconnecting device of Level-1 and Level-2 areas.

The IS-IS interface level attributes are also divided into the following three types:

- Level-1 attribute interface: it can only send and receive Level-1 packet of IS-IS and only establish a neighbor of Level-1;
- Level-2 attribute interface: it can only send and receive Level-2 packet of IS-IS and only establish a neighbor of Level-2;
- Level-1-2 attribute interface: it can send and receive the Level-1 and Level-2 packets of IS-IS simultaneously and establish the neighbors of Level-1 and Level-2 simultaneously.

The IS-IS interface level attributes rely on IS-IS global level attributes. The Level-1 intermediate system can only own the interfaces of Level-1 attributes, the Level-2 intermediate system can only own the interfaces of Level-2 attributes, and the Level-1-2 intermediate system can own the interfaces of all attributes.

Table 43-4 Configure IS-IS Global Level Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure IS-IS global level attribute	**is-type { level-1 | level-1-2 | level-2-only }**	Optional By default, IS-IS global level attribute is Level-1-2

Table 43-5 Configure IS-IS Interface Level Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure interface level attribute	**isis circuit-type [level-1 | level-1-2 | level-2]**	Optional By default, when the interface level attribute is not specified, it is identical to the global level attribute

NOTE

- There may be only one Level-2 IS-IS process in the same VRF.

43.2.3 Configure IS-IS Route Generation *-E -A*

Configuration Conditions

Before configuring IS-IS route generation, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible.
- Enable IS-IS protocol.

Configure IS-IS Default Route

The Level-2 area of the IS-IS protocol cannot generate a default route during running. You can add a default route (the route with the destination address of 0.0.0.0/0) message in the Level-2 LSP and advertise it. Areas of the same level in other intermediate systems will add a default route to the routing table after receiving this message.

Table 43-6 Configure IS-IS Default Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Enter IS-IS IPv4 address family configuration mode	**address-family ipv4 unicast**	-
Configure IS-IS to advertise the default route	**default-information originate**	Required By default, no default route is advertised

Configure IS-IS Route Re-distribution

Through the route Re-distribution, the route information of the other routing protocols can be introduced to IS-IS, so that the AS running the IS-IS protocol is interconnected to the AS or routing domain running other routing protocols. When introducing an external route, you can specify the policy for the route introduction and the level attributes of the introduced route.

Table 43-7 Configure IS-IS Route Re-distribution

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Enter IS-IS IPv4 address family configuration mode	**address-family ipv4 unicast**	-
Configure IS-IS route Re-distribution	**redistribute** *protocol* [*protocol-id*] [**level-1** / **level-1-2** / **level-2** / **metric** *metric-value* / **metric-type** { **external** | **internal** } / **route-map** *route-map-name* / **match** *route-sub-type*]	Required By default, the information about other routing protocols is not Re-distributed.

43.2.4 Configure IS-IS Route Control *-E -A*

Configuration Conditions

Before configuring the IS-IS route features, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible.
- Enable IS-IS protocol.

Configure IS-IS Metric Style

The original IS-IS only had a narrow metric style. When the narrow metric style was used, the maximum metric value of the interface is 63. With the gradual expansion of network size, the narrow metric style had been far from meeting the needs; later, the metric style was extended and the wide metric style was added, with the metric value up to 16777214; devices with different metric styles cannot advertise and learn route information to and from each other. In order to achieve the transition between the two metric styles, a configuration method for the transition metric styles is provided.

The wide metric style is recommended.

Table 43-8 Configure IS-IS Metric Style

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure the interface metric style	**metric-style** {**narrow** | **narrow transition** | **transition** | **wide** | **wide transition**} [**level-1** | **level-1-2** | **level-2**]	Optional By default, the narrow metric style is used.

Configure IS-IS Interface Metric Value

After the IS-IS protocol is enabled, the metric of the IS-IS route is the global metric value. You may specify the metric value for each interface separately through the command.

Table 43-9 Configure the Interface Metric Value

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure the IS-IS global metric value	**metric** *metric-value* **[level-1 | level-2]**	Optional By default, the global metric value is 10.

Steps	Command	Description
Return to the global configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the interface metric value	**isis ipv4 metric** {*metric-value* | **maximum**} [**level-1** | **level-2**]	Optional By default, the global metric value is used.

Configure the Administrative Distance of IS-IS

The system prefers the route according to the administrative distance, the smaller the administrative distance, the more preferential the route.

Table 43-10 Configure the Administrative Distance of IS-IS

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Enter IS-IS IPv4 address family configuration mode	**address-family ipv4 unicast**	-
Configure the administrative distance of IS-IS route	**distance** *distance-value*	Optional By default, the administrative distance is 115.

Configure IS-IS Route Summary

The route summary is to summarize multiple routes as a route. After the route summary is configured for IS-IS, it can effectively reduce the advertisements of the number of accessible subnets and reduce the size of the link state database and routing table, thus effectively saving memory and CPU resources. This configuration is typically used on Level-1-2 border devices to reduce the route information advertised among the levels.

Table 43-11 Configure IS-IS Route Summary

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Enter IPv4 address family configuration mode	**address-family ipv4 unicast**	-
Configure IS-IS route summary	**summary-prefix** *prefix-value* [**metric** *metric-value* **/ route-type** {**internal | external**} **/ metric-type {internal | external**} **/ tag** *tag-value* **/ not-advertise / level-1 / level-2 / level-1-2]**	Required By default, the route summary is not performed.

Configure the Maximum Number of IS-IS Load Balancing Entries

There can be multiple paths with the same cost to the same destination address. Through these equivalent paths, link utilization can be improved, and the user can control the maximum number of equivalent routes of IS-IS.

Table 43-12 Configure the Maximum Number of IS-IS Load Balancing Entries

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Enter IPv4 address family configuration mode	**address-family ipv4 unicast**	-
Configure the maximum number of IS-IS load balancing entries	**maximum-paths** *max-number*	Optional By default, the maximum number of load balancing entries is 4

Configure IS-IS Inter-level Route Leakage

By default, IS-IS will only leak the Level-1 routes to Level-2 and the routes in Level-2 area cannot known in Level-1 area. The inter-level route leakage can be configured to introduce Level-2 routes to Level-1 area. In configuring the inter-level route leakage, you may specify a route policy that only the routes matching the conditions are leaked.

Table 43-13 Configure IS-IS Inter-level Route Leakage

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Enter IS-IS IPv4 address family configuration mode	**address-family ipv4 unicast**	-
Configure IS-IS inter-level route leakage	**propagate** { **level-1 into level-2** | **level-2 into level-1** } [**distribute-list** *access-list-name* | **route-map** *route-map-name*]	Required By default, Level-1 leaks routes to Level-2.

Configure IS-IS ATT Bit

In the Level-1-2 device, the ATT bit is used to advertise other nodes that whether the local node is connected to other areas. If so, ATT bit will be automatically set to 1 and the other nodes will generate a default route to the local node, which will increase the service burden of the local node. To prevent this, ATT bit can be forced to 0.

Table 43-14 Configure IS-IS ATT Bit

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Enter IS-IS IPv4 address family configuration mode	**address-family ipv4 unicast**	-
Configure IS-IS ATT bit	**set-attached-bit** { **on** | **off** }	Required By default, ATT bit is set according to whether the node is connected to other areas.

43.2.5 Configure IS-IS Network Optimization ***-E -A***

Configuration Conditions

Before configuring IS-IS adjustment and optimization, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible.

- Enable IS-IS protocol.

Configure IS-IS Interface Priority

On the broadcast link, IS-IS needs to elect a node as DIS, which sends CSNP packets periodically and synchronizes the link state databases of the whole network; the DIS nodes of Level-1 and Level-2 are elected respectively, the ones with the highest interface priority are elected as DIS nodes, and the ones with the same priority and large MAC addresses are elected as DIS nodes.

Table 43-15 Configure IS-IS Interface Priority

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure IS-IS interface priority	**isis priority** *priority-value* [**level-1** | **level-2**]	Optional By default, the interface priority is 64

Configure a passive IS-IS interface

On a passive interface, the IS-IS protocol packets are not sent and received, but the direct network route information is still published; by configuring a passive interface, IS-IS can save the bandwidth and CPU processing time; on this configuration basis, you can also specify that IS-IS only publishes the direct network route information for the passive interface instead of the direct network route information for non-passive interfaces.

Table 43-16 Configure a Passive IS-IS Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure a passive IS-IS interface	**passive-interface** *interface-name*	Required By default, IS-IS has no passive interface
Configure IS-IS to publish the route information of the passive interface only	**advertise-passive-only**	Optional By default, all direct network route information

Steps	Command	Description
		with IS-IS interface enabled is published.

Configure IS-IS Hello Packet Parameters

1. Configure Hello send interval

The interface with IS-IS protocol enabled will send the Hello packet periodically to maintain adjacency with neighbors. The smaller the send interval of Hello packet is, the faster the network converges, but the larger the bandwidth is.

Table 43-17 Configure Hello Send Interval

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the Hello send interval on the interface	**isis hello-interval** { *interval* | **minimal** } [**level-1** | **level-2**]	Optional By default, the Hello send interval is 10s

2. Configure the number of Hello packet failures

IS-IS calculates the neighborship holdtime according to the number of Hello packet failures and advertises the holdtime to the neighbor device. If the neighbor device does not receive the Hello packet in this period, the neighborship fails and the route will be recomputed.

Table 43-18 Configure the Number of Hello Packet Failures

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the number of Hello packet failures on the interface	**isis hello-multiplier** *multiplier* [**level-1** | **level-2**]	Optional By default, the number of Hello packet failures is 3

3. Configure to disable Hello packet padding

To prevent inconsistent MTU values of the interfaces at both ends of the link from leading to passage of only small packets, IS-IS pads the Hello packet to the interface MTU value, so that it cannot establish neighborship; but this method results in a waste of bandwidth. In practice, it can be configured to send a miniaturized Hello packet without padding the Hello packet.

Table 43-19 Configure to Disable Hello Packet Padding

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Disable Hello packet padding	**no isis hello padding**	Required By default, Hello packet padding is enabled.

Configure IS-IS LSP Packet Parameters

1. Configure the maximum lifetime of LSP packet

Each LSP packet has a maximum survival time. When the survival time of LSP packet decreases to zero, it will be deleted from the link state database. The maximum lifetime of LSP packet shall be greater than the refresh interval of LSP packet.

Table 43-20 Configure IS-IS LSP Packet Parameters

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure the maximum lifetime of LSP packet	**max-lsp-lifetime** *life-time*	Optional By default, the maximum lifetime of LSP packet is 1200s

2. Configure the refresh interval of LSP packet

The IS-IS protocol advertises and learns the routes by interacting with the LSP packets, the node stores the received LSP packets in its own link state database and each LSP packet has a maximum lifetime, so each node shall regularly update its LSP packet to prevent the maximum lifetime of LSP packet from decreasing to zero and keep the LSP packets in the whole area in sync. Reducing the LSP packet send interval can accelerate the convergence speed of the network, but will take up more bandwidth.

Table 43-21 Configure the Refresh Interval of LSP Packet

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure the refresh interval of LSP packet	**lsp-refresh-interval** *refresh-interval*	Optional By default, the periodical send interval is 900s

3. Configure the generation interval of LSP packet

In addition to periodic updates, the interface state changes and network state changes will trigger the generation of new LSP packets. To prevent the frequent generation of LSP packets from consuming a large amount of CPU resources, the user can configure the minimum generation interval of LSP packets.

Table 43-22 Configure the Generation Interval of LSP Packet

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure the generation interval of LSP packet	**lsp-gen-interval** [**level-1** | **level-2**] *max-interval* [*initial-interval* [*secondary-interval*]]	Optional By default, the maximum generation interval of LSP packets is 10s and the minimum generation interval is 50ms.

4. Configure the send interval of LSP packet

Every time an LSP packet is generated, it will be sent on the interface. In order to prevent the frequent generation of LSP packets from consuming a large amount of interface bandwidth, you can configure the minimum send interval of LSP packet for each interface.

Table 43-23 Configure the Send Interval of LSP Packet

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the send interval of LSP packet	**isis lsp-interval** *min-interval*	Optional By default, the send interval of LSP packet is 33ms

5. Configure the retransmit interval of LSP packet

On the point-to-point link, IS-IS needs to send PSNP acknowledgment message to the peer end after sending an LSP packet. If no acknowledgment message from the peer end is received, the LSP packet will be sent again. The time for awaiting acknowledgment, i.e. the retransmit time of LSP packet, can be configured by the user to prevent the retransmission of LSP packet due to failure to receive acknowledgment under long time delay.

Table 43-24 Configure the Retransmit Interval of LSP Packet

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the retransmit interval of LSP packet	**isis retransmit-interval** *interval* [**level-1** | **level-2**]	Optional By default, the retransmit interval is 5s.

6. Configure LSP MTU value

The packets of the IS-IS protocol cannot be fragmented automatically. in order not to affect the normal spread of LSP packets, it is required that the maximum length of LSP packets in a routing domain should not exceed the minimum MTU value of IS-IS interface of all devices; so when the MTU value of the device interfaces in the routing domain is inconsistent, it is recommended to uniformly set the maximum length of LSP packets.

Table 43-25 Configure LSP MTU Value

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-

Steps	Command	Description
Configure LSP MTU value	**lsp-mtu** *mtu-size* [**level-1** | **level-2**]	Optional By default, the LSP MTU value is 1492 bytes

Configure IS-IS SNP Packet Parameters

1. Configure the send interval of CSNP packet

In the broadcast link election node, you need to send the CSNP packets periodically to synchronize the whole network link state database. The periodic send interval of CSNP packet can be adjusted according to the actual situation.

Table 43-26 Configure the Send Interval of CSNP Packet

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the send interval of CSNP packet	**isis csnp-interval** *interval* [**level-1** | **level-2**]	Optional By default, the periodical send interval of CSNP packet is 10s.

2. Configure the send interval of PSNP packet

On the broadcast link, the PSNP packet is used to synchronize the whole network link state database, and on point-to-point link, PSNP packet is used to confirm the received LSP packet. In order to prevent a large number of PSNP packets from being sent on the interface, a minimum send interval is set for PSNP packets, which can be dynamically modified by the user. The send interval of PSNP packet should not be set too large; otherwise, it will affect the synchronization of the whole network link state database for the broadcast link and will result in retransmission of the LSP packet for point-to-point link due to the failure to receive the acknowledgment in time.

Table 43-27 Configure the Send Interval of PSNP Packet

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the send interval of PSNP packet	**isis psnp-interval** *min-interval* [**level-1** | **level-2**]	Optional

Steps	Command	Description
		By default, the send interval of PSNP packet is 2s

Configure IS-IS SPF Computing Interval

The change in the IS-IS link state database will trigger SPF route computation and frequent SPF computation will consume a lot of CPU resources. The user may configure the SPF computing interval.

Table 43-28 Configure IS-IS SPF Computing Interval

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Enter IS-IS IPv4 address family configuration mode	**address-family ipv4 unicast**	-
Configure IS-IS SPF computing interval	**spf-interval** [**level-1** | **level-2**] *maximum-interval* [*min-initial-delay* [*min-second-delay*]]	Optional

Configure IS-IS Maximum Area Number

Multiple area addresses may be configured in an IS-IS process for smooth transition of multiple Level-1 areas into a Level-1 area or a Level-1 area into multiple Level-1 areas.

Table 43-29 Configure IS-IS Maximum Area Number

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure IS-IS maximum area number	**max-area-addresses** *max-number*	Optional By default, the maximum area address number is 3.

NOTE

- This configuration requires consistent configuration in the entire IS-IS Level-1 routing domain, otherwise Level-1 neighbors will not be established normally, and for Level-2 neighbors, there will be no impact.

Configure IS-IS Hostname Mapping

IS-IS uniquely identifies an intermediate system through the system ID, which has a fixed length of 6 bytes. When viewing the system information (neighborship, link state database, etc.), the user cannot visually link the system ID with the hostname information; IS-IS supports the mapping of system ID and hostname, making it more intuitive and convenient for the user to query the system information. There are two ways to configure the IS-IS hostname mapping:

1. Configure IS-IS static hostname mapping

IS-IS static hostname mapping is where the user manually creates a system ID and hostname for a remote device.

Table 43-30 Configure IS-IS Static Hostname Mapping

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure IS-IS static hostname mapping	**hostname static** *system-id host-name*	Required

2. Configure IS-IS dynamic hostname mapping

The static hostname mapping requires the user to configure the system ID and hostname mapping of other devices for each device in the network; while the dynamic hostname mapping only enables the hostname advertisement once the hostname is configured for each device, so that other devices in the network can learn the hostname of that device.

Table 43-31 Configure IS-IS dynamic hostname mapping

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure IS-IS dynamic hostname mapping	**hostname dynamic** { *host-name* | **area-tag** | **recv-only** | **system-name** }	Required

Steps	Command	Description
		By default, only the hostname advertised by other devices is learnt.

Configure IS-IS Interface to Join Mesh Group

Before joining Mesh group, the IS-IS interface will send an LSP packet from an interface via all other IS-IS interfaces, resulting in a large bandwidth waste in a full mesh connected network; several IS-IS interfaces can be added to the same Mesh group, and when the interface receives the LSP packet, it will only send the LSP packet to the interface that is not in the same Mesh group as the interface.

Table 43-32 Configure IS-IS Interface to Join Mesh Group

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure IS-IS interface to join Mesh group	**isis mesh-group** { *group-number* | **blocked** }	Required By default, it does not join Mesh group.

NOTE

- **isis mesh-group blocked** sets the interface to a blocking interface. The blocking interface will not send LSP packets actively, and only send an LSP packet when receiving an LSP request.

43.2.6 Configure IS-IS Network Authentication *-E -A*

Configuration Conditions

Before configuring the IS-IS network authentication, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible.
- Enable IS-IS protocol.

Configure IS-IS Neighbor Authentication

After configuring IS-IS to enable neighborship authentication, an authentication message will be added to the Hello packet sent, and the Hello packet received will be authenticated. If the authentication fails, the neighborship will not be formed, which can prevent the establishment of neighborship with untrustworthy devices.

Table 43-33 Configure IS-IS Neighbor Authentication

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the authentication mode of Hello packet	**isis authentication mode** { **md5** | **text** } [**level-1** | **level-2**]	Required By default, the authentication function is disabled
Configure the authentication key of Hello packet	**isis authentication key** { **0** | **7** } *password* [**level-1** | **level-2**]	To be selected alternatively By default, no authentication key is available; the authentication key may be configured using a key chain, which is described in the key chain configuration section of the manual.
	isis authentication key-chain *key-chain-name* [**level-1** | **level-2**]	

Configure IS-IS Route Authentication

After configuring IS-IS route information authentication, an authentication message will be added to the LSP and SNP packets and the LSP and SNP packets received will be authenticated. If the authentication fails, the packets will be directly discarded, which can prevent untrusted route information from spreading to the IS-IS network.

Table 43-34 Configure IS-IS Route Authentication

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure the authentication mode of route information packet	**authentication mode** { **md5** | **text** } [**level-1** | **level-2**]	Required By default, the authentication function is disabled

Steps	Command	Description
Configure the authentication key of route information packet	**authentication key** { **0** | **7** } *password* [**level-1** | **level-2**]	To be selected alternatively By default, no authentication key is available; the authentication key may be configured using a key chain, which is described in the key chain configuration section of the manual.
	authentication key-chain *key-chain-name* [**level-1** | **level-2**]	

43.2.7 Configure IS-IS to Link with BFD -E -A

Configuring IS-IS to link with BFD can quickly detect the link faults and enable the backup link for communication. There are two ways to configure IS-IS to link with BFD: all interfaces with enabled IS-IS protocol are associated with BFD; the specified interface is associated with BFD.

For BFD parameter information, refer to BFD configuration manual.

Configuration Conditions

Before configuring IS-IS to link with BFD, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible.
- Enable IS-IS protocol.

Configure IS-IS to Link with BFD

Table 43-35 Configure IS-IS to Link with BFD

Steps	Command
Enter global configuration mode	**configure terminal**
Enter the interface configuration mode	**interface** *interface-name*
Configure the interface to enable BFD link detection	**isis bfd**
Return to the global configuration mode	**exit**
Enter the IS-IS configuration mode	**router isis** [*area-tag*]
Configure all IS-IS interfaces to enable BFD link detection	**bfd all-interfaces**

43.2.8 Configure IS-IS GR -E -A

GR (Graceful Restart) is used to keep the route information at the forwarding level of the local device and neighbor device unchanged and the forwarding not affected during the master-backup switching; after the device switching and re-running, the two devices synchronize the route information at the protocol level and update the forward layer, so as to achieve the purpose of uninterrupted data forwarding during the switching process.

There are two roles in the GR process:

- GR Restarter end - a device that performs protocol GR.
- GR Helper end - a device that helps the protocol GR.

Distributed devices can serve as GR Restarter and GR Helper, while centralized devices can only serve as GR Helper to assist the Restarter end to complete GR.

Configuration Conditions

Before configuring IS-IS GR, ensure that:

- The IP address of the interface is configured to make the adjacent node network layers accessible.
- Enable IS-IS protocol.

Configure IS-IS GR Restarter

Table 43-36 Configure IS-IS GR Restarter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure IS-IS to enable GR	**nsf ietf**	Required By default, the GR function is disabled
Configure advertisement of the retransmit times of messages entering GR process	**nsf interface-expire** *resend-cnt*	Optional By default, the number of retransmit times is 3
Configure the retransmit waiting time of messages entering GR process	**nsf interface-timer** *wait-time*	Optional By default, the waiting time is 10s

Configure IS-IS GR Helper

The GR Helper helps the Restarter complete GR. By default, the device enables the function and the user disables the function by a command.

Table 43-37 Configure IS-IS GR Helper

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IS-IS configuration mode	**router isis** [*area-tag*]	-
Configure IS-IS GR Helper to disable Helper	**nsf ietfhelper-disable**	Required Configure IS-IS GR Helper to disable Helper

43.2.9 IS-IS Monitoring and Maintaining

-E -A

Table 43-38 IS-IS Monitoring and Maintaining

Command	Description
clear isis [**instance -null** | *area-tag*] **statistics** [*interface_name*]	Clear IS-IS protocol running statistics
clear isis [**instance -null** | *area-tag*] **process**	Restart IS-IS protocol process
show isis [**instance -null** | *area-tag*]	Show the information about IS-IS process
show isis instance { **-null** | *area-tag* } **bfd-sessions**	Show the information about BFD sessions of IS-IS process
show isis [**instance** -null | *area-tag*] **database** [*lsp_id*] [**detail**] [**l1** / **l2**] [**level-1** / **level-2**] [**self**] [**verbose**]	Show the information about the link state database of IS-IS
show isis interface [*interface-name*] [**detail**]	Show the information about the interface running IS-IS protocol
show isis [**instance –null** | *area-tag*] **ipv4 reach-info**	Show IPV4 subnet accessible information of IS-IS
show isis [**instance –null** | *area-tag*] **ipv4 route**	Show IPV4 route information of IS-IS

Command	Description
show isis [**instance –null** | *area-tag*] **ipv4 topology**	Show the information about IPV4 topology of IS-IS
show isis [**instance – null** | *area-tag*] **is-reach-info** [**level-1** | **level-2**]	Show information about neighbor nodes of IS-IS
show isis [**instance –null** | *area-tag*] **mesh-groups**	Show the mesh groups of IS-IS
show isis [**instance –null** | *area-tag*] **neighbors** [*interface-name*] [**detail**]	Show the neighbors of IS-IS
show isis [**instance –null** | *area-tag*] **statistics** [*interface-name*]	Show IS-IS protocol running statistics
show isis router	Show IS-IS hostname information

43.3 IS-IS Typical Configuration Example

43.3.1 Configure Basic Functions of IS-IS *-E -A*

Network Requirements

- Configure IS-IS protocol to interconnect the devices.
- Device1 is Level-1 router and Device2 is Level-1-2 router. Both Device1 and Device2 are in area 10. Device3 is Level-2 router in area 20. Device2 connects two areas.

Network Topology

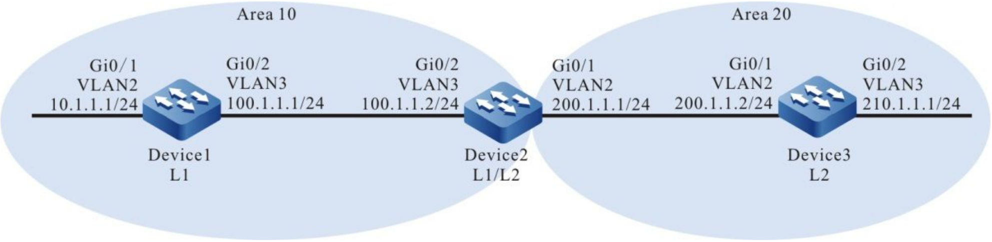


Figure 43-1 Networking for Configuring the Basic Functions of IS-IS

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Configure IS-IS and enable the process in the interface.

#Device1 configures IS-IS process 100 with the type of Level-1 in area 10 and enables the process in the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#Device2 configures IS-IS process 100 with the type of Level-1-2 in area 10 and enables the process in the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#Device3 configures IS-IS process 100 with the type of Level-2 in area 20 and enables the process in the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

Step 3: Check the result.

#Query the IS-IS neighbor information of Device1.

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type   System ID      Interface       State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3       Up    29 sec   L1    capable  64       0000.0000.0001.01
```

#Query the IS-IS neighbor information of Device2.

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type   System ID      Interface       State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2       Up    9 sec    L2    capable  64       0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3       Up    8 sec    L1    capable  64       0000.0000.0001.01
```

Device2 establish an IS-IS neighbor with Device1 and Device3 respectively.

#Query the IS-IS neighbor information of Device3.

```
Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type   System ID      Interface       State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan3       Up    22 sec   L2    capable  64       0000.0000.0003.01
```

#Query the route information of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is 100.1.1.2 to network 0.0.0.0

i   0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C   10.1.1.0/24 is directly connected, 4:56:18 PM, vlan2
C   100.1.1.0/24 is directly connected, 6:37:57 PM, vlan3
C   127.0.0.0/8 is directly connected, 284:2:13 AM, lo0
i   200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
    via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 10.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan2
L1 100.1.1.0/24, flags none, metric 10, from network connected
```

```
    via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
    via 100.1.1.2, vlan3, neighbor 0000.0000.0002
```

Device1 has a default route in its routing table, with Device2 as the next hop.

#Query the route information of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i   10.1.1.0/24 [115/20] via 100.1.1.1, 4:58:26 PM, vlan3
C   100.1.1.0/24 is directly connected, 6:39:58 PM, vlan3
C   127.0.0.0/8 is directly connected, 8:16:34 PM, lo0
C   200.1.1.0/24 is directly connected, 6:39:37 PM, vlan2
i   210.1.1.0/24 [115/20] via 200.1.1.2, 4:57:56 PM, vlan2

Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
    via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
    via 200.1.1.2, vlan2, neighbor 0000.0000.0003
```

Device2 contains the routes Level-1 and Level-2.

#Query the route information of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i   10.1.1.0/24 [115/30] via 200.1.1.1, 4:59:29 PM, vlan2
i   100.1.1.0/24 [115/20] via 200.1.1.1, 5:47:29 PM, vlan2
C   127.0.0.0/8 is directly connected, 945:29:12, lo0
C   200.1.1.0/24 is directly connected, 6:40:27 PM, vlan2
C   210.1.1.0/24 is directly connected, 4:59:04 PM, vlan3
```

```
Device3#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 30, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 100.1.1.0/24, flags none, metric 20, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
```

Device3 learns Level-1 route and Level-1 leaks to Level-2 by default.

NOTE

- The metric style is narrow metric by default. The wide metric is recommended.
- By default, IS-IS entity attribute is Level-1-2.

43.3.2 Configure IS-IS DIS Election *-E -A*

Network Requirements

- Specify the device as DIS by modifying the priority.
- Device1 and Device2 are Level-1-2 devices, Device3 is Level-1 device and Device4 is Level-2 device. Device1, Device2, Device3 and Device4 are in the same broadcast network and in the same area 10.

Network Topology

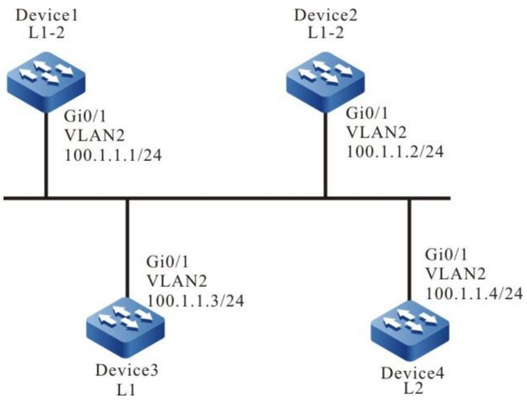


Figure 43-2 Networking for Configuring IS-IS DIS Election

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Configure IS-IS and enable the process in the interface.

#Device1 configures IS-IS process 100 with the type of Level-1-2 in area 10 and enables the process in the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
```

#Device2 configures IS-IS process 100 with the type of Level-1-2 in area 10 and enables the process in the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
```

#Device3 configures IS-IS process 100 with the type of Level-1 in area 10 and enables the process in the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-1
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
```

#Device4 configures IS-IS process 100 with the type of Level-2 in area 20 and enables the process in the interface.

```
Device4#configure terminal
Device4(config)#router isis 100
Device4(config-isis)#net 20.0000.0000.0004.00
Device4(config-isis)#is-type level-2
```

```
Device4(config-isis)#metric-style wide
Device4(config-isis)#exit
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ip router isis 100
Device4(config-if-vlan2)#exit
```

#Query the IS-IS neighbor information of Device1.

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 4):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan2       Up    23 sec   L1    capable  64       0000.0000.0003.01
L2-LAN 0000.0000.0002 vlan2       Up    23 sec   L2    capable  64       0000.0000.0004.01
L1-LAN 0000.0000.0003 vlan2       Up    8 sec    L1    capable  64      0000.0000.0003.01
L2-LAN 0000.0000.0004 vlan2       Up    8 sec    L2    capable  64      0000.0000.0004.01
```

The pseudo-node of Level-1 is 0000.0000.0003.01 and Device3 is Level-1 DIS. The pseudo-node of level-2 is 0000.0000.0004.01 and Device4 is Level-2 DIS.

#Use the command **show isis interface** to query the MAC address of the interface. In the default priority, the selection of DIS is based on the principle that the larger the MAC address of the physical interface, the higher the priority.

Step 3: Modify the interface priority.

#Modify the interface priority of Device1.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#isis priority 100
Device1(config-if-vlan2)#exit
```

Step 4: Check the result.

#Query the IS-IS neighbor information of Device1.

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 4):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan2       Up    24 sec   L1    capable  64       0000.0000.0001.01
L2-LAN 0000.0000.0002 vlan2       Up    23 sec   L2    capable  64       0000.0000.0001.01
L1-LAN 0000.0000.0003 vlan2       Up    20 sec   L1    capable  64       0000.0000.0001.01
L2-LAN 0000.0000.0004 vlan2       Up    24 sec   L2    capable  64       0000.0000.0001.01
```

The pseudo-node of Level-1-2 is 0000.0000.0001.01 and Device1 is Levev-1-2 DIS.

NOTE

- By default, IS-IS interface priority is 64, the greater the value, the higher the priority.

43.3.3 Configure IS-IS Inter-level Route Leakage -E -A

Network Requirements

- Leak Level-2 route to Level-1 by configuring the inter-level leakage on Level-1-2 device.
- Device1 is Level-1 router and Device2 is Level-1-2 router. Both Device1 and Device2 are in area 10. Device3 is Level-2 router in area 20. Device2 connects two areas.

Network Topology

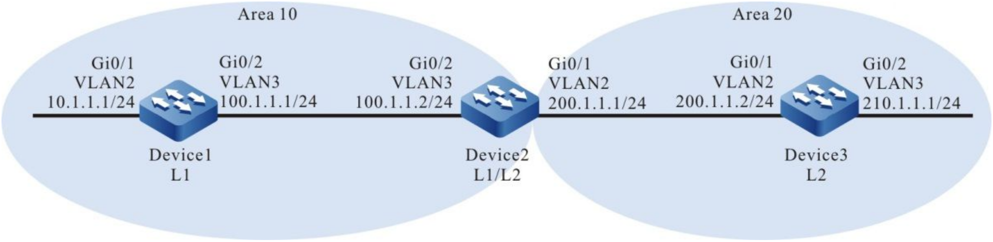


Figure 43-3 Networking for IS-IS Inter-level Leakage

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Configure IS-IS and enable the process in the interface.

#Device1 configures IS-IS process 100 with the type of Level-1 in area 10 and enables the process in the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#Device2 configures IS-IS process 100 with the type of Level-1-2 in area 10 and enables the process in the interface.

```
Device2#configure terminal
```

```
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#Device3 configures IS-IS process 100 with the type of Level-2 in area 20 and enables the process in the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

#Query the route information of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is 100.1.1.2 to network 0.0.0.0

i   0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C   10.1.1.0/24 is directly connected, 4:56:18 PM, vlan2
C   100.1.1.0/24 is directly connected, 6:37:57 PM, vlan3
C   127.0.0.0/8 is directly connected, 284:2:13 AM, lo0
i   200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
```

```
    via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 10.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan2
L1 100.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
    via 100.1.1.2, vlan3, neighbor 0000.0000.0002

Device1#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime   Length  ATT/P/OL
0000.0000.0001.00-00* 0x0000007E   0xD5DA        1067          71      0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.1
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 10.1.1.0/24
  Metric: 10         IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000073   0xAAAF        471           51      0/0/0
  Metric: 0          IS-Extended 0000.0000.0001.00
  Metric: 0          IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00  0x00000081   0x5926        887           71      1/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 200.1.1.1
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 100.1.1.0/24
  Metric: 10         IP-Extended 200.1.1.0/24
```

There is a default route in the routing table, with Device2 as the next hop, and there is no Level-2 route advertised by Device3.

#Query the route information of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i   10.1.1.0/24 [115/20] via 100.1.1.1, 16:58:26,vlan3
C   100.1.1.0/24 is directly connected, 6:39:58 PM, vlan3
C   127.0.0.0/8 is directly connected, 8:16:34 PM, lo0
```

```
C   200.1.1.0/24 is directly connected, 6:39:37 PM, vlan2
i   210.1.1.0/24 [115/20] via 200.1.1.2, 4:57:56 PM, vlan2

Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
     via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
     via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
     via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
     via 200.1.1.2, vlan2, neighbor 0000.0000.0003

Device2#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime   Length  ATT/P/OL
0000.0000.0001.00-00  0x0000007E   0xD5DA        507            71      0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.1
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 10.1.1.0/24
  Metric: 10         IP-Extended 100.1.1.0/24
0000.0000.0001.01-00  0x00000074   0xA8B0        799            51      0/0/0
  Metric: 0          IS-Extended 0000.0000.0001.00
  Metric: 0          IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000082   0x5727        1146           71      1/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 200.1.1.1
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 100.1.1.0/24
  Metric: 10         IP-Extended 200.1.1.0/24

IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime   Length  ATT/P/OL
0000.0000.0002.00-00* 0x00000081   0x84C0        1047           79      0/0/0
  NLPID: IPv4
  Area Address: 10
```

```
 IP Address: 200.1.1.1
 Metric: 10        IS-Extended 0000.0000.0003.01
 Metric: 20        IP-Extended 10.1.1.0/24
 Metric: 10        IP-Extended 100.1.1.0/24
 Metric: 10        IP-Extended 200.1.1.0/24
0000.0000.0003.00-00  0x00000315   0x9DC7       543          71      0/0/0
 NLPID: IPv4
 Area Address: 20
 IP Address: 210.1.1.1
 Metric: 10        IS-Extended 0000.0000.0003.01
 Metric: 10        IP-Extended 200.1.1.0/24
 Metric: 10        IP-Extended 210.1.1.0/24
0000.0000.0003.01-00  0x00000070   0xBF97       526          51      0/0/0
 Metric: 0        IS-Extended 0000.0000.0002.00
 Metric: 0        IS-Extended 0000.0000.0003.00
```

Device2 contains the routes Level-1 and Level-2.

#Query Device3 route information. Device3 contains Level-1 route advertised by Device1.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i   10.1.1.0/24 [115/30] via 200.1.1.1, 4:59:29 PM, vlan2
i   100.1.1.0/24 [115/20] via 200.1.1.1, 5:47:29 PM, vlan2
C   127.0.0.0/8 is directly connected, 945:29:12, lo0
C   200.1.1.0/24 is directly connected, 6:40:27 PM, vlan2
C   210.1.1.0/24 is directly connected, 4:59:04 PM, vlan3

Device3#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 30, from learned, installed
    via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 100.1.1.0/24, flags none, metric 20, from learned, installed
    via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 200.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan3
```

```
Device3#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID               LSP Seq Num  LSP Checksum  LSP Holdtime   Length  ATT/P/OL
0000.0000.0002.00-00  0x00000081   0x84C0       880           79      0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 200.1.1.1
  Metric: 10         IS-Extended 0000.0000.0003.01
  Metric: 20         IP-Extended 10.1.1.0/24
  Metric: 10         IP-Extended 100.1.1.0/24
  Metric: 10         IP-Extended 200.1.1.0/24
0000.0000.0003.00-00* 0x00000316   0x9BC8       1197          71      0/0/0
  NLPID: IPv4
  Area Address: 20
  IP Address: 210.1.1.1
  Metric: 10         IS-Extended 0000.0000.0003.01
  Metric: 10         IP-Extended 200.1.1.0/24
  Metric: 10         IP-Extended 210.1.1.0/24
0000.0000.0003.01-00* 0x00000070   0xBF97       359           51      0/0/0
  Metric: 0         IS-Extended 0000.0000.0002.00
  Metric: 0         IS-Extended 0000.0000.0003.00
```

Step 3: Configure the inter-level leakage.

#Device2 configures the inter-level leakage.

```
Device2(config)#router isis 100
Device2(config-isis)#address-family ipv4 unicast
Device2(config-isis-af)#propagate level-2 into level-1
Device2(config-isis-af)#exit
Device2(config-isis)#exit
```

Step 4: Check the result.

#Query the route information of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is 100.1.1.2 to network 0.0.0.0
```

```
i   0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C   10.1.1.0/24 is directly connected, 4:56:18 PM, vlan2
C   100.1.1.0/24 is directly connected, 6:37:57 PM, vlan3
C   127.0.0.0/8 is directly connected, 284:2:13 AM, lo0
i   200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3
i   210.1.1.0/24 [115/30] via 100.1.1.2, 12:00:01 AM, vlan3

Device1#show isis ipv4 route
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
     via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 100.1.1.0/24, flags none, metric 10, from network connected
     via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
     via 100.1.1.2,vlan3, neighbor 0000.0000.0002
L1 210.1.1.0/24, flags inter-area, metric 30, from learned, installed
     via 100.1.1.2, vlan3, neighbor 0000.0000.0002

Device1#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime   Length  ATT/P/OL
0000.0000.0001.00-00* 0x0000007F   0xD3DB        668            71      0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.1
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 10.1.1.0/24
  Metric: 10         IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000075   0xA6B1        995            51      0/0/0
  Metric: 0          IS-Extended 0000.0000.0001.00
  Metric: 0          IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00  0x00000083   0x4DA6        984            79      1/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 200.1.1.1
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 100.1.1.0/24
  Metric: 10         IP-Extended 200.1.1.0/24
  Metric: 20         IP-Extended ia 210.1.1.0/24
```

In addition to the default route, Device1 also learns the Level-2 route advertised by Device3.

43.3.4 IS-IS Route Re-distribution

-E -A

Network Requirements

- Configure Re-distribution to introduce the internal routes to IS-IS to achieve networking between devices.
- Device1 and Device2 are Level-2 routers. Configure IS-IS in area 10. Device2 and Device3 configure OSPF. On Device2, Re-distribute the OSPF route to IS-IS.

Network Topology

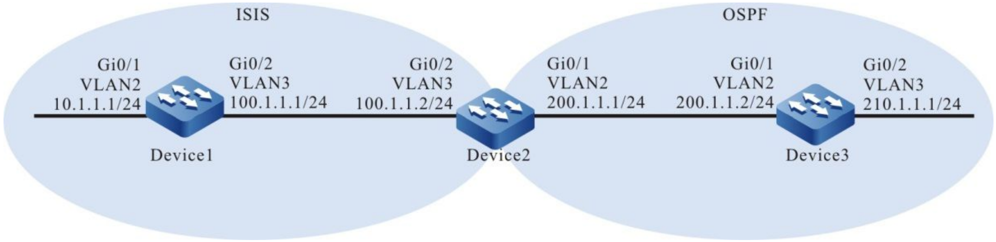


Figure 43-4 Networking for IS-IS Route Re-distribution

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Configure IS-IS and enable the process in the interface.

#Device1 configures IS-IS process 100 with the type of Level-2 in area 10 and enables the process in the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#Device2 configures IS-IS process 100 with the type of Level-1-2 in area 10 and enables the process in the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
```

```
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

Step 3: Configure OSPF.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#network 200.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 210.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 200.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device1. Device1 does not learn the OSPF route Re-distributed by Device2.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 12:58:39 AM, vlan2
C   100.1.1.0/24 is directly connected, 6:55:35 AM, vlan3
C   127.0.0.0/8 is directly connected, 603:6:22 AM, lo0

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3

Device1#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime   Length  ATT/P/OL
0000.0000.0001.00-00* 0x00000046   0x489E        1123           71      0/0/0
```

```
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.1
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 10.1.1.0/24
  Metric: 10         IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000045   0x097D        1103           51      0/0/0
  Metric: 0          IS-Extended 0000.0000.0001.00
  Metric: 0          IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00  0x000000CB   0xEEA6        679            63      0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.2
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 100.1.1.0/24
```

#Query the routing table of Device2. Device2 learns ISIS and OSPF routes.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i   10.1.1.0/24 [115/20] via 100.1.1.1, 3:45:37 PM, vlan3
C   100.1.1.0/24 is directly connected, 10:38:58 PM, vlan3
C   127.0.0.0/8 is directly connected, 300:3:03 AM, lo0
C   200.1.1.0/24 is directly connected, 10:38:58 PM, vlan2
O   210.1.1.1/32 [110/2] via 200.1.1.2, 3:43:35 PM, vlan2

Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 20, from learned, installed
     via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L2 100.1.1.0/24, flags none, metric 10, from network connected
     via 0.0.0.0, vlan3

Device2#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime   Length  ATT/P/OL
0000.0000.0001.00-00  0x00000046   0x489E        911            71      0/0/0
  NLPID: IPv4
```

```
 Area Address: 10
 IP Address: 100.1.1.1
 Metric: 10        IS-Extended 0000.0000.0001.01
 Metric: 10        IP-Extended 10.1.1.0/24
 Metric: 10        IP-Extended 100.1.1.0/24
0000.0000.0001.01-00  0x00000045   0x097D       892          51      0/0/0
 Metric: 0        IS-Extended 0000.0000.0001.00
 Metric: 0        IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00* 0x000000CB   0xEEA6       467          63      0/0/0
 NLPID: IPv4
 Area Address: 10
 IP Address: 100.1.1.2
 Metric: 10        IS-Extended 0000.0000.0001.01
 Metric: 10        IP-Extended 100.1.1.0/24
```

Step 4: Configure IS-IS to Re-distribute the OSPF route.

#On Device2, Re-distribute the OSPF route to IS-IS Level-2.

```
Device2(config)#router isis 100
Device2(config-isis)#address-family ipv4 unicast
Device2(config-isis-af)#redistribute ospf 100 level-2
Device2(config-isis-af)#exit
Device2(config-isis)#exit
```

Step 5: Check the result.

#Query the route information of Device1. Device1 learns the OSPF route Re-distributed by Device2.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 4:47:30 PM, vlan2
C   100.1.1.0/24 is directly connected, 10:44:27 PM, vlan3
C   127.0.0.0/8 is directly connected, 618:55:13, lo0
i   200.1.1.0/24 [115/10] via 100.1.1.2, 12:00:05 AM, vlan3
i   210.1.1.1/32 [115/10] via 100.1.1.2, 12:00:05 AM, vlan3

Device1#show isis ipv4 route
```

```
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan2
L2 100.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan3
L2 200.1.1.0/24, flags none, metric 10, from learned, installed
    via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L2 210.1.1.1/32, flags none, metric 10, from learned, installed
    via 100.1.1.2, vlan3, neighbor 0000.0000.0002


Device1#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime   Length  ATT/P/OL
0000.0000.0001.00-00* 0x00000046   0x489E       626           71      0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.1
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 10.1.1.0/24
  Metric: 10         IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000045   0x097D       606           51      0/0/0
  Metric: 0         IS-Extended 0000.0000.0001.00
  Metric: 0         IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00  0x000000CD   0xC6E2       1184          80      0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.2
  Metric: 10         IS-Extended 0000.0000.0001.01
  Metric: 10         IP-Extended 100.1.1.0/24
  Metric: 0         IP-Extended 200.1.1.0/24
  Metric: 0         IP-Extended 210.1.1.1/32
```

Device1 learns the Re-distributed OSPF route.

43.3.5 Configure IS-IS Neighbor Authentication -E -A

Network Requirements

- Enable neighbors between devices with the same key by enabling authentication on the interface.
- Device1 is Level-1 router and Device2 is Level-1-2 router. Both Device1 and Device2 are in area 10. Device3 is Level-2 router in area 20. Device2 connects two areas.

Network Topology

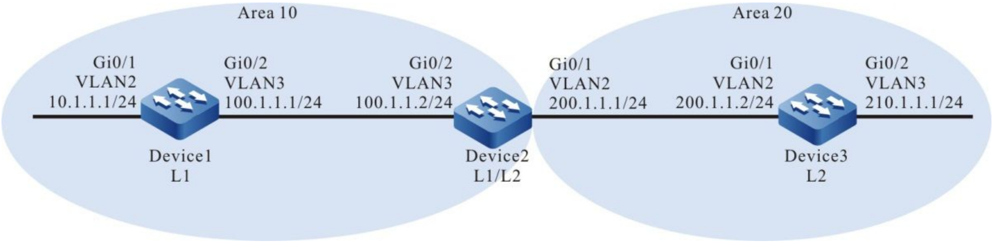


Figure 43-5 Networking for IS-IS Neighbor Authentication

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Configure IS-IS and enable the process in the interface.

#Device1 configures IS-IS process 100 with the type of Level-1 in area 10 and enables the process in the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#Device2 configures IS-IS process 100 with the type of Level-1-2 in area 10 and enables the process in the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#Device3 configures IS-IS process 100 with the type of Level-2 in area 20 and enables the process in the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

#Query the IS-IS neighbor information of Device1.

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3            Up    29 sec   L1    capable  64       0000.0000.0001.01
```

#Query the IS-IS neighbor information of Device2.

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2            Up    9 sec    L2    capable  64       0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3            Up    7 sec    L1    capable  64       0000.0000.0001.01
```

#Query the IS-IS neighbor information of Device3.

```
Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan2            Up    24 sec   L2    capable  64       0000.0000.0003.01
```

Step 3: Configure authentication.

#Configure MD5 authentication on Device2 interface, with the password of admin.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#isis authentication mode md5
Device2(config-if-vlan2)#isis authentication key 0 admin
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#isis authentication mode md5
Device2(config-if-vlan3)#isis authentication key 0 admin
```

```
Device2(config-if-vlan3)#exit
```

#Query the IS-IS neighbor of Device2.

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 0):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
```

Device1 and Device3 have not yet been configured for authentication, and Device2 has not established an ISIS neighbor.

#On vlan3 of Device1, configure MD5 authentication with the password of admin.

```
Device1(config)#interface vlan3
Device1(config-if-vlan3)#isis authentication mode md5
Device1(config-if-vlan3)#isis authentication key 0 admin
Device1(config-if-vlan3)#exit
```

#On vlan2 of Device3, configure MD5 authentication with the password of admin.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#isis authentication mode md5
Device3(config-if-vlan2)#isis authentication key 0 admin
Device3(config-if-vlan2)#exit
```

Step 4: Check the result.

#Query the IS-IS neighbor information of Device1.

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3       Up    29 sec   L1    capable  64       0000.0000.0001.01
```

You can see that Device1 has successfully established an ISIS neighbor with Device2, indicating successful authentication.

#Query the IS-IS neighbor information of Device2.

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2       Up    9 sec    L2    capable  64      0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3       Up    7 sec    L1    capable  64      0000.0000.0001.01
```

You can see that Device2 has successfully established ISIS neighbors with Device1 and Device3, indicating successful authentication.

#Query the IS-IS neighbor information of Device3.

```
Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type   System ID      Interface        State Holdtime Level IETF-NSF Priority Circuit ID
```

```
L2-LAN 0000.0000.0002 vlan2      Up    24 sec   L2    capable  64      0000.0000.0003.01
```

You can see that Device3 has successfully established an ISIS neighbor with Device2, indicating successful authentication.

#Query the route information of Device2. It can normally receive the routes advertised by Device1 and Device3.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i   10.1.1.0/24 [115/20] via 100.1.1.1, 4:58:26 PM, vlan3
C   100.1.1.0/24 is directly connected, 6:39:58 PM, vlan3
C   127.0.0.0/8 is directly connected, 8:16:34 PM, lo0
C   200.1.1.0/24 is directly connected, 6:39:37 PM, vlan2
i   210.1.1.0/24 [115/20] via 200.1.1.2, 4:57:56 PM, vlan2

Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
    via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
    via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
    via 200.1.1.2, vlan2, neighbor 0000.0000.0003
```

43.3.6 Configure IS-IS to Link with BFD *-E -A*

Network Requirements

- Configure BFD between the devices. When the main line fails, the service can quickly switch to the backup line.
- Device1, Device2 and Device3 are Level-2 routers in the same area 10. Configure BFD in Device1 and Device3 to establish a session. When the line between Device1 and Device3 is disconnected abnormally, Device1 can switch quickly and learn the route 10.1.1.1/24 from Device2.

Network Topology

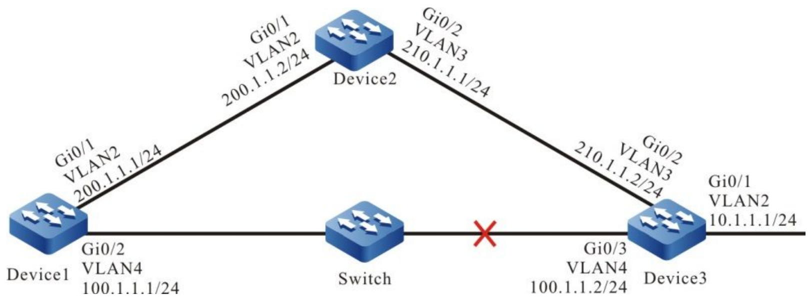


Figure 43-6 Networking for IS-IS to Link with BFD

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Configure IS-IS and enable the process in the interface.

#Device1 configures IS-IS process 100 with the type of Level-2 in area 10 and enables the process in the interface.

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if- vlan2)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip router isis 100
Device1(config-if-vlan4)#exit
```

#Device2 configures IS-IS process 100 with the type of Level-2 in area 10 and enables the process in the interface.

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
```

```
Device2(config-if-vlan3)#exit
```

#Device3 configures IS-IS process 100 with the type of Level-2 in area 10 and enables the process in the interface.

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan4
Device3(config-if-vlan4)#ip router isis 100
Device3(config-if-vlan4)#exit
```

#Query the route information of Device1. Device1 prefers the route 10.1.1.0/24 advertised by Device3.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS


Gateway of last resort is not set


i   10.1.1.0/24 [115/20] via 100.1.1.2, 12:00:15 AM, vlan4
C   100.1.1.0/24 is directly connected, 12:09:15 AM, vlan4
C   127.0.0.0/8 is directly connected, 253:58:17, lo0
C   200.1.1.0/24 is directly connected, 12:11:29 AM, vlan2
i   210.1.1.0/24 [115/20] via 100.1.1.2, 12:00:15 AM, vlan4
             [115/20] via 200.1.1.2, 12:00:15 AM, vlan2
Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.2, vlan4, neighbor 0000.0000.0003
L2 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan4
L2 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
```

```
    via 100.1.1.2, vlan4, neighbor 0000.0000.0003
    via 200.1.1.2, vlan2, neighbor 0000.0000.0002
```

Step 3:   Configure BFD.

#Enable BFD on the interface of Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan4
Device1(config-if-vlan4)#isis bfd
Device1(config-if-vlan4)#exit
#Enable BFD on the interface of Device3.
Device3(config)#bfd fast-detect
Device3(config)#interface vlan4
Device3(config-if-vlan4)#isis bfd
Device3(config-if-vlan4)#exit
```

#Query the BFD information of Device1.

```
Device1#show bfd session
OurAddr            NeighAddr           LD/RD          State
100.1.1.2          100.1.1.1           1/1          UP
Holddown           interface
5000             vlan4
```

Step 4:   Check the result.

#After a fault occurs on the line between Device1 and Device3, BFD will quickly detect the default and advertise to ISIS. ISIS will switch the route to Device2 for communication. Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i   10.1.1.0/24 [115/30] via 200.1.1.2, 12:00:14 AM, vlan2
C   127.0.0.0/8 is directly connected, 112:55:25, lo0
C   200.1.1.0/24 is directly connected, 101:8:08 PM, vlan2

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 30, from l earned, installed
```

```
    via 200.1.1.2, vlan2, neighbor 0000.0000.0003
L2 200.1.1.0/24, flags none, metric 20, from network connected
    via 0.0.0.0, vlan2
```

#As you can see, the data streams from Device1 to the network segment 10.1.1.0/24 take precedence over Device2.

44 BGP

44.1 Overview

BGP (Border Gateway Protocol) is a routing protocol used between the AS (Autonomous System) to exchange NLRI (Network Layer Reachability Information). The IGP (Internal Gateway Protocol), such as RIP, OSPF and IS-IS, focuses on finding the exact path, with network nodes (router, three-layer switch, multi-network card host, etc.) as the pathfinding unit, while EGP (External Gateway Protocol) focuses on controlling the routing direction, with AS as the unit.

BGP is applied to the interconnection between AS networks and provides the route information exchange between AS. It is mostly used for large network convergence and network core. This application level determines that BGP has the following characteristics compared with IGP:

- BGP uses TCP protocol to transmit packets and the service port number is 179. TCP guarantees the reliability of transmission, so BGP does not need to design a transmission control strategy to ensure the reliability of information;
- BGP updates the route in the incremental form, that is, only when the route attributes change or a route is added/deleted will it advertise to the neighbors, which greatly reduces the network bandwidth occupied by the BGP propagation route;
- BGP is a distance vector protocol based on AS and solves the routing loops by carrying AS path attributes in the route packets;
- BGP route has a wealth of attributes, which can be modified by applying routing policies to achieve free control of route filtration and selection;
- The neighbor type of BGP can be iBGP or eBGP, each neighbor can be assigned different route policy.

44.2 BGP Function Configuration

Table 44-1 BGP Function List

Configuration task	
Configure a BGP neighbor	Configure an IBGP neighbor
	Configure an EBGP neighbor
	Configure a passive BGP neighbor

Configuration task	
	Configure an MP-BGP neighbor
	Configure BGP neighbor MD5 authentication
Configure BGP route generation	Configure BGP to advertise the local route
	Configure BGP route Re-distribution
	Configure BGP to advertise the default route
Configure BGP route control	Configure BGP to advertise an aggregate route
	Configure the administrative distance of BGP route
	Configure route policy for the outgoing direction of BGP neighbor
	Configure route policy for the incoming direction of BGP neighbor
	Configure the maximum number of route entries received from BGP neighbor
	Configure the maximum number of BGP load balancing entries
Configure BGP route attributes	Configure BGP route weight
	Configure MED attribute of BGP route
	Configure Local-Preference attribute of BGP route
	Configure AS_PATH attribute of BGP route
	Configure NEXT-HOP attribute of BGP route
	Configure BGP route community attributes
Configure BGP network optimization	Configure BGP neighbor Keepalive time
	Configure BGP route scan time
	Configure EBGP neighbor fast failover

Configuration task	
	Configure BGP route suppression
	Configure BGP neighbor refresh capability
	Configure BGP neighbor soft-reconfiguration capability
	Configure BGP neighbor ORF capability
Configure BGP large network	Configure BGP peer group
	Configure BGP route reflector
	Configure BGP confederation
Configure BGP GR	Configure BGP GR Helper
Configure BGP to link with BFD	Configure EBGP to link with BFD
	Configure IBGP to link with BFD

44.2.1 Configure a BGP Neighbor *-E -A*

Configuration Conditions

Before configuring a BGP neighbor, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer;
- The network layer address of the interface is configured to make the adjacent node network layers accessible;

Configure an IBGP Neighbor

1. Basic configuration

Configuring the IBGP neighbor requires specifying the neighbor AS to be the same AS the device AS. The device can be configured with a Router ID that uniquely identifies a BGP device when establishing a BGP session. When Router ID is not configured, it will be selected by the device according to the interface address. The priority principle is as follows:

- Select the largest IP address of the Loopback interface as the Router ID;
- If the Loopback interface of IP address is not configured, select the largest IP address from other interfaces as the Router ID;
- Only when the interface is in the UP state can the interface address be selected as the Router ID.

Table 44-2 Configure an IBGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable BGP and enter the BGP configuration mode	**router bgp** *autonomous-system*	Required By default, BGP is disabled
Configure BGP device ID	**bgp router-id** *router-id*	Optional By default, the device selects the ID according to the interface address in line with the principle of Loopback address priority and large IP address priority.
Configure an IBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no IBGP neighbor is created
Enable IBGP neighbor to send and receive IPv4 unicast route	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**	Optional By default, IBGP neighbor is automatically enabled to send and receive IPv4 unicast route
Configure IBGP neighbor description	**neighbor** { *neighbor-address* | *peer-group-name* } **description** *description-string*	Optional By default, IBGP neighbor is not described

2. Configure the source address of TCP session

BGP uses TCP as its transport protocol. Characterized by reliable transport, TCP effectively ensures that BGP packets can be correctly transmitted to the neighbor.

Table 44-3 Configure the Source Address of TCP Session

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enable BGP and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure an IBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no IBGP neighbor is created
Configure the source address of IBGP neighbor TCP session	**neighbor** { *neighbor-address* | *peer-group-name* } **update-source** { *interface-name* | *ip-address* }	Required By default, the address of the route output interface is automatically selected as the source address of the TCP session.

NOTE

- The source address of TCP session needs to be explicitly configured between BGP neighbors in the presence of load balanced route. When the TCP source address is not configured, the BGP session may not be successfully established for a period of time due to the fact that the optimal route of the neighbors is different and different output interfaces are used as their respective source addresses.

Configure an EBGP Neighbor

1. Basic configuration

Configuring the EBGP neighbor requires specifying the neighbor AS that is different from the device AS.

Table 44-4 Configure an EBGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable BGP and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure an EBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no EBGP neighbor is created

2. Configure a Non-direct EBGP neighbor

EBGP neighbors are in different operating networks and are usually connected by a direct physical link, so the default TTL value of IP packets for communication between EBGP neighbors is 1. The TTL value of the IP packets can be set by configuring a command between non-direct operating networks to connect BGP.

Table 44-5 Configure a Non-direct EBGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure an EBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no EBGP neighbor is created
Configure the source address of EBGP neighbor TCP session	**neighbor** { *neighbor-address* | *peer-group-name* } **update-source** { *interface-name* | *ip-address* }	Optional By default, the address of the route output interface is automatically selected as the source address of the TCP session.
Configure to allow connection between EBGP neighbors	**neighbor** { *neighbor-address* | *peer-group-name* } **ebgp-multihop** [*ttl-value*]	Required By default, EBGP neighborship is not allowed between non-direct devices

Configure a Passive BGP Neighbor

The passive neighbor function of BGP is required for special applications. After applying the passive neighbor, the BGP does not initiate the TCP connection request to the neighbor to establish an BGP neighbor, and can only wait for the neighbor to initiate the connection request. By default, the neighbors will initiate connections with each other, and in the event of a conflict, a TCP connection will be preferred to form a BGP session. Before configuring a passive BGP neighbor, you need to configure a BGP neighbor.

Table 44-6 Configure a Passive BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a BGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no BGP neighbor is created.
Configure a passive BGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **passive**	Required By default, no passive neighbor is enabled

Configure an MP-BGP Neighbor

By default, a BGP neighbor is activated to send and receive IPv4 unicast routes by default under the IPv4 unicast address family shall be activated through configuration commands under the other address families to send and receive corresponding routes, such as multicast address family, VRF address family, LS unicast address family, etc. Before configuring an MP-BGP neighbor, you need to configure a BGP neighbor.

Table 44-7 Configure an MP-BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a BGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no BGP neighbor is created.
Enter the BGP IPv4 multicast configuration mode	**address-family ipv4 multicast**	Required By default, it is in unicast address family mode after entering BGP configuration mode
Activate the neighbor under the BGP IPv4 multicast address family	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**	Required By default, no global neighbor is activated

Steps	Command	Description
		under the multicast address family
Exit the BGP IPv4 multicast configuration mode	**exit-address-family**	-
Enter the BGP IPv4 VRF configuration mode	**address-family ipv4 vrf** *vrf-name*	-
Configure a neighbor under the BGP IPv4 address family	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no BGP neighbor is created.
Activate the neighbor under the IPv4 VRF address family	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**	Optional By default, the neighbor in the BGP IPv4 VRF configuration mode has been activated
Exit the BGP IPv4 VRF configuration mode	**exit-address-family**	-
Enter the BGP LS configuration mode	**address-family link-state unicast**	-
Activate the neighbor under the BGP LS unicast address family	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**	Required By default, no global neighbor is activated under the VPN address family
Exit the BGP LS configuration mode	**exit-address-family**	-

NOTE

- A neighbor configured in BGP configuration mode and BGP IPv4 unicast configuration mode is a global neighbor, and a neighbor configured in BGP IPv4 VRF configuration mode belongs only to the VRF address family.

Configure BGP Neighbor MD5 Authentication

BGP supports configuring MD5 authentication, which is done by TCP transport protocol, to protect information interactions between neighbors. Neighbors must have the same MD5 authentication key to establish a TCP connection, otherwise a TCP connection cannot be established after the MD5 authentication failure by the TCP transport protocol. Before configuring the BGP neighbor MD5 authentication, you need to configure a BGP neighbor.

Table 44-8 Configure BGP Neighbor MD5 Authentication

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a BGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no BGP neighbor is created.
Configure BGP neighbor MD5 authentication	**neighbor** { *neighbor-address* | *peer-group-name* } **password** [0 | 7] *password-string*	Required By default, MD5 authentication is not made between BGP neighbors.

44.2.2 Configure BGP Route Generation -E -A

Configuration Conditions

Before configuring the BGP route generation, ensure that:

- Enable BGP;
- Configure a BGP neighbor and establish a session successfully.

Configure BGP to Advertise the Local Route

BGP can introduce a route from the IP routing table to the BGP routing table through the **network** command. The route is introduced into the BGP routing table and published only if there are entries in the IP routing table that match the **network** prefix and mask exactly.

When publishing a local route, you can either apply a route map to the route or specify the route as a backdoor route. The backdoor route treats an EBGP route as a local BGP route and uses the administrative distance of the local route to allow the IGP route to take precedence over the EBGP route, while the backdoor route is not advertised to the EBGP neighbor.

Table 44-9 Configure BGP to Advertise the Local Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to advertise the local route	**network** *ip-address mask* [**route-map** *rtmap-name* [**backdoor**] | **backdoor**]	Required By default, BGP does not advertise any local route

NOTE

- BGP advertises a local route with the route Origin attribute type of IGP.
- After applying the **network backdoor** command on the EBGP route, the administrative distance of the EBGP route will become that of the local route (by default, the administrative distance of EBGP route is 20 and of the local route is 200) and less than the default administrative distance of the IGP route, so that the IGP route is preferred and a backdoor link is formed between EBGP neighbors.
- The match options supported by the route map that is applied by BGP to advertise the local route include as-path, community, extcommunity, ip address, ip nexthop and metric, and the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin and weight.

Configure BGP Route Re-distribution

BGP is not primarily responsible for learning the route, but rather for controlling the route direction by managing the route attributes, so BGP generates a BGP route to advertise to the neighbor by redistributing the IGP. While redistributing the IGP route, BGP may apply the route map.

Table 44-10 Configure BGP Route Re-distribution

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to Re-distribute RIP routes	**redistribute** { **connected** | **irmp** *as-number* | **isis** [*area-tag*] [**match** *isis-level*] | **ospf** *as-number*	Required

Steps	Command	Description
	[**match** *route-sub-type*] | **rip** | **static** } [**route-map** *map-name* / **metric** *value*]	By default, BGP does not Re-distribution any other IGP route

NOTE

- BGP advertises an IGP route with the route Origin attribute type of INCOMPLETE.
- The match options supported by the route map that is applied by BGP to Re-distribute other protocols include as-path, community, extcommunity, ip address, ip nexthop and metric, and the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin and weight.

Configure BGP to Advertise the Default Route

BGP needs to introduce the default route before advertising it to a neighbor. There are two ways to introduce the default route: generate the default route through the **neighbor default-originate** command; Re-distribute the default route of other protocols through the **default-information originate** command.

The default route generated through the **neighbor default-originate** command is a route 0.0.0.0/0 automatically generated through BGP and the default route Re-distributed through the **default-information originate** command is a route 0.0.0.0/0 introduced by BGP to a Re-distributed protocol.

Table 44-11 Configure BGP to advertise the Default Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to generate the default route	**neighbor** { *neighbor-address* | *peer-group-name* } **default-originate** [**route-map** *rtmap-name*]	Required By default, BGP does not generate the default route
Configure BGP to Re-distribute the default route of other protocols	**default-information originate**	Required By default, BGP does not Re-distribute the default route of other protocols

NOTE

- You also need to configure the route Re-distribution while configure BGP to Re-distribute the default route of other protocols.
- You may apply the route map to the default route when configuring BGP to generate the default route.
- The set options supported by the route map that is applied by BGP to generate the default route include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin and weigh.

44.2.3 Configure BGP Route Control *-E -A*

Configuration Conditions

Before configuring the BGP route control, ensure that:

- Enable BGP;
- Configure a BGP neighbor and establish a session successfully.

Configure BGP to Advertise an Aggregate Route

In a large BGP network, you need to configure a BGP aggregate route to reduce the number of routes advertised to the neighbor or to effectively control the BGP routing process.

Table 44-12 Configure BGP to advertise an aggregate route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to advertise an aggregate route	**aggregate-address** *ip-address mask* [**as-set** / **summary-only** / **route-map** *rtmap-name*]	Required By default, BGP will not perform route aggregation.

NOTE

- When BGP advertises an aggregate route, you can reduce the size of the route advertisements by specifying the summary-only command option to advertise only the aggregate route.
- An aggregate route with the AS_PATH attribute can be generated by specifying the as-

set command option.

- You may set richer attributes of the aggregate route by applying the route map to the aggregate route.

Configure the Administrative Distance of BGP Route

In the IP routing table, each protocol has an administrative distance to control routing, the smaller the value, the higher the priority. BGP influences the routing by configuring the administrative distance to the specified network segment. The administrative distance covering the route to the specified network segment will be modified. Meanwhile, ACL can be applied to effectively filter the covered network segment. Only the administrative distance that the ACL allows for network segments is modified.

The **distance bgp** command is used to modify the administrative distance of the external and internal routes of BGP and the local routes, while the **distance** command is only used to modify the administrative distance of the routes in the specified network segments. The **distance** command takes precedence over the **distance bgp** command. A network segment covered by the **distance** will use the administrative distance specified by the command, while an uncovered network segment will use the administrative distance set by **distance bgp**.

Table 44-13 Configure the Administrative Distance of BGP Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to modify the default administrative distance	**distance bgp** *external-distance internal-distance local-distance*	Optional By default, the administrative distance of EBGP route is 20, of IBGP route is 200 and of local route is 200.
Configure the administrative distance for a specified network segment	**distance** *administrative-distance ip-address mask* [*acl-name*]	

Configure Route Policy for the Outgoing Direction of BGP Neighbor

The BGP route advertisement or routing is accomplished by its powerful route attributes. When advertising routes to a neighbor, you may modify the route attributes by corresponding policies or filter some routes. The policies currently supported for application in the outgoing direction are:

- distribute-list;
- filter-list: filter-list of AS_PATH properties;
- prefix-list: IP prefix-list;
- Route-map: Route Map.

Table 44-14 Configure Route Policy for the Outgoing Direction of BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Specify the distribute-list to be applied in the outgoing direction	**neighbor** { *neighbor-address* | *peer-group-name* } **distribute-list** *access-list-name* **out**	Multiple choice (the distribute-list and IP prefix-list cannot be configured simultaneously) By default, the route policy for the outgoing direction of BGP neighbor is not configured.
Specify the AS_PATH attribute filter-list to be applied in the outgoing direction	**neighbor** { *neighbor-address* | *peer-group-name* } **filter-list** *aspath-list-name* **out**	
Specify the IP prefix-list to be applied in the outgoing direction	**neighbor** { *neighbor-address* | *peer-group-name* } **prefix-list** *prefix-list-name* **out**	
Specify the route map to be applied in the outgoing direction	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **out**	

NOTE

- The route policy configured for the outgoing direction of BGP neighbor can take effect only after the neighbor is set.
- When configuring the route map applied in the outgoing direction of the route reflector, you can only change the NEXT-HOP attributes.
- Refer to the PBR Tools -Configure AS-PATH list to configure the filter-list.
- Multiple policies can be configured in the outgoing direction of the neighbor simultaneously and applied by BGP in the sequential order of **distribute-list**, **filter-list**, **prefix-list** and **route-map**. After the first policy is rejected, the next policy is not applied, and the route information is not advertised until all the configured policies have passed.
- The match options supported by the route map that is applied in the outgoing direction of BGP include as-path, community, extcommunity, ip address, ip nexthop and metric, and the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin and weight.

Configure Route Policy for the Incoming Direction of BGP Neighbor

BGP can apply policies to filter or modify the attributes of received route information. Like the outgoing direction, the incoming direction also supports four policies:

- distribute-list;
- filter-list: filter-list of AS_PATH properties;
- prefix-list: IP prefix-list;
- Route-map: Route Map.

Table 44-15 Configure Policy for the Incoming Direction of BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Specify the distribute-list to be applied in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **distribute-list** *access-list-name* **in**	Multiple choice (the distribute-list and IP prefix-list cannot be configured simultaneously) By default, no policy is specified in the incoming direction
Specify the AS_PATH attribute filter-list to be applied in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **filter-list** *aspath-list-name* **in**	
Specify the IP prefix-list to be applied in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **prefix-list** *prefix-list-name* **in**	
Specify the route map to be applied in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in**	

NOTE

- The route policy configured for the incoming direction of BGP neighbor can take effect only after the neighbor is set.
- Multiple policies can be configured in the incoming direction of the neighbor simultaneously and applied by BGP in the sequential order of **distribute-list**, **filter-list**, **prefix-list** and **route-map**. After the first policy is rejected, the next policy is not applied, and the route is added to the database only all configured policies have passed.
- The match options supported by the route policy that is applied in the incoming direction of BGP include as-path, community, extcommunity, ip address, ip nexthop and metric, and the set options supported include as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin and weight.

Configure the Maximum Number of Route Entries Received from BGP Neighbor

The BGP device supports limiting the number of route entries received from a specified neighbor and gives an alarm or is disconnected when the number of routes received from the specified neighbor reaches a certain threshold.

Table 44-16 Configure the Maximum Number of Route Entries Received from BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the maximum number of route entries received from a neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **maximum-prefix** *prefix-num* [*threshold-value*] [**warning-only**]	Required By default, the number of prefix entries received from a neighbor is not limited.

NOTE

- If the warning-only command option is not specified, when the number of routes received by a neighbor by BGP reaches the maximum number of entries, the BGP session will be disconnected automatically.
- If the warning-only command option is specified, when the number of routes received by a neighbor by BGP reaches the maximum number of entries, BGP gives a warning message only and does not prevent the routes from continuing to learn.

Configure the Maximum Number of BGP Load Balancing Entries

In a BGP networking environment, if there are several paths with the same overhead to the same destination, a load balanced route can be formed by configuring the number of BGP load entries.

Table 44-17 Configure the Maximum Number of BGP Load Balancing Entries

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-

Steps	Command	Description
Configure the maximum number of IBGP load balancing entries	**maximum-paths ibgp** *number*	Required By default, IBGP does not perform the load balanced routing
Configure the maximum number of EBGP load balancing entries	**maximum-paths** *number*	Required By default, EBGP does not perform the load balanced routing

NOTE

- After the maximum number of BGP load balancing entries is configured, the load can be formed only when the EBGP route is preferred.
- The command for the configuration of the maximum number of load balancing entries is different in different BGP configuration modes, as shown in the description of the **maximum-paths** in BGP technical manual.

44.2.4 Configure BGP Route Attributes *-E -A*

Configuration Conditions

Before configuring the BGP route attributes, ensure that:

- Enable BGP;
- Configure a BGP neighbor and establish a session successfully.

Configure BGP Route Weight

The first rule for BGP routing is to compare the weight value of the routes. The greater the weight value of the route, the higher the priority. The route weight value is a local attribute of the device and is not passed to other BGP neighbors. The route weight values range from 0 to 65535. By default, the weight value of the routes learnt from a neighbor is 0 and of all routes generated by the local device is 32768.

Table 44-18 Configure BGP Route Weight

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-

Steps	Command	Description
Configure the route weight of a neighbor or peer group	**neighbor** { *neighbor-address* | *peer-group-name* } **weight** *weight-num*	Required By default, the route weight of a neighbor is 0

Configure MED Attribute of BGP Route

The MED attribute is used to select the best route for traffic entering AS. Under the same routing conditions, when BGP learns the routes with the same destination but different next hop from different EBGP neighbors, it will prefer the route with the minimum MED as the best entry.

MED is sometimes referred to as an "external metric" and is marked as "Metric" in the BGP routing table. BGP will advertise the MED attributes of the route learnt from the neighbor to the IBGP neighbors, but not to the EBGP neighbors, so MED is only applicable between the neighbor AS.

1. Configure BGP to compare MED of the routes from different AS neighbors

By default, BGP will only perform MED routing for routes learnt from the same AS, but can ignore the restrictions on the same AS requirements in MED routing through the command **bgp always-compare-med**.

Table 44-19 Configure BGP to Compare MED of the Routes from Different AS Neighbors

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to compare MED of the routes from different AS neighbors	**bgp always-compare-med**	Required By default, BGP is only allowed to compare the MED of routes from the same AS.

2. Configure BGP to sort MED according to the route grouping by AS_PATH

By default, MED sorting by BGP according to the route grouping by AS_PATH is disabled. This function can be enabled through the command **bgp deterministic-med**. In route selection, all routes are arranged based on AS_PATH. In each AS_PATH group, the routes are sorted according to the size of MED. The route with the smallest MED value is selected as the best route of this group.

Table 44-20 Configure BGP to Sort MED according to the Route Grouping by AS_PATH

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
BGP sorts MED according to the route grouping by AS_PATH	**bgp deterministic-med**	Required By default, MED sorting by BGP according to the route grouping by AS_PATH is disabled.

3. Configure to compare MED of routes in the local confederation

EBGP routes from different AS do not compare MED attributes by default. This principle is also valid for the EBGP in the confederation. The command **bgp bestpath med confed** is used to compare the MED attribute value of the routes in the local confederation.

Table 44-21 Configure BGP to Compare MED of Routes in the Local Confederation

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to compare MED attribute value of routes in the local confederation	**bgp bestpath med confed**	Required By default, the MED attribute value of routes in the local confederation will not be compared.

4. Configure a route map to modify MED attribute

When receiving and sending routes, you can use the route map to modify the MED attribute value.

Table 44-22 Configure a Route Map to Modify MED Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a route map to modify MED attribute	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in | out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the MED attribute, you need to modify MED through the **set metric** command. See PBR Tools - Technical manual -**set metric**.
- After configuring the command **neighbor attribute-unchanged**, you cannot change the neighbor MED attribute through the route map.

Configure Local-Preference Attribute of BGP Route

The Local-Preference attribute is passed only between IBGP neighbors. Local-Preference is used to select the best exit from AS, and the route with the largest Local-Preference will be preferred.

The Local-Preference value ranges from 0 to 4294967295, the higher the value, the higher the priority of the route. By default, the Local-Preference attribute of all routes advertised to the IBGP neighbors is 100 and the Local-Preference attribute can be modified through **bgp default local-preference** or road map.

1. Configure BGP to modify the default Local-Preference attribute

Table 44-23 Configure BGP to Modify the Default Local-Preference Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the default Local-Preference attribute of BGP	**bgp default local-preference** *local-value*	Optional By default, the default local priority is 100.

2. Configure a route map to modify the Local-Preference attribute

Table 44-24 Configure a Route Map to Modify the Local-Preference Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a route map to modify the Local-Preference attribute	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in | out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the Local-Preference attribute, you need to modify Local-Preference attribute through the command **set local-preference**. See PBR Tools - Technical manual -**set local-preference**.

Configure AS_PATH Attribute of BGP Route

1. Configure to ignore AS_PATH comparison in BGP routing

Under other same conditions, the route with the shortest AS_PATH will be preferred in the BGP routing, but the routing through AS_PATH can be canceled through the command **bgp bestpath as-path ignore**.

Table 44-25 Configure to Ignore AS_PATH Comparison in BGP Routing

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to ignore AS_PATH comparison in BGP routing	**bgp bestpath as-path ignore**	Required By default, AS_PATH attribute value is compared in routing.

2. Configure the number of repeats of local AS number allowed by BGP

To avoid routing loops, BGP will check the AS_PATH attribute of the routes received from the neighbors and discard the routes containing local AS number. Through the command **neighbor allowas-in**, the routes received by BGP are allowed to contain the local AS number in the AS_PATH attribute and the number of routes containing the local AS number may be configured.

Table 44-26 Configure the Number of Repeats of Local AS Number Allowed by BGP

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the number of repeats of local AS number	**neighbor** { *neighbor-address* | *peer-group-name* } **allowas-in** [*as-num*]	Required By default, a route received from a neighbor is not allowed to have a local AS number in the AS_PATH attribute

3. Configure to remove private AN number when BGP advertises routes to neighbors

In a large BGP network, the route AS_PATH attribute has a confederation or community attribute. By default, BGP will carry this private AS attribute information when it advertises to its neighbors. To block the private network information, you may remove the private AS number through **neighbor remove-private-AS**.

Table 44-27 Configure to Remove Private AN Number when BGP Advertises Routes to Neighbors

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to remove private AN number when BGP advertises routes to neighbors	**neighbor** { *neighbor-address* | *peer-group-name* } **remove-private-AS**	Required By default, BGP will carry a private AS number when it

Steps	Command	Description
		advertises to its neighbors.

4. Configure to detect the validity of the first AS number of EBGP route

When BGP advertises a route to an EBGP neighbor, the local AS number is pressed into the start position of AS_PATH. The first AS that advertises the route will be at the last position. Normally, the first AS number of the route received from EBGP should be the same as the neighbor's AS number, or the route will be discarded.

Table 44-28 Configure to Detect The Validity of the First AS Number of EBGP Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to detect the validity of the first AS number of EBGP route	**bgp enforce-first-as**	Required By default, this first AS number check mechanism is disabled for BGP.

5. Configure a route map to modify the AS_PATH attribute

BGP supports to configure a route map to modify the AS_PATH attribute. The route attributes may be prepended through **set as-path prepend**, so as to affect the neighbor routing. In using **set as-path prepend**, the local AS is preferred to prepend AS_PATH. If another AS is used, enough attention must be paid to avoid the route advertisements to that AS being rejected.

Table 44-29 Configure a Route Map to Modify the AS_PATH Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a route map to modify the AS_PATH attribute	**neighbor** { *neighbor-address* | *peer-group-name* }	Required

Steps	Command	Description
	route-map *rtmap-name* **in | out**	By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the AS_PATH attribute, you need to modify the AS_PATH attribute through the command **set as-path prepend**. See PBR Tools - Technical manual - **set as-path**.

Configure NEXT-HOP Attribute of BGP route

When BGP advertises a route to an IBGP neighbor, the route attributes will not be changed (including next-hop attribute). When BGP advertises the route learnt from an EBGP neighbor to an IBGP neighbor, the next-hop attribute of the route advertised to the BGP neighbor is the local IP address through the command **neighbor next-hop-self**. BGP also supports the use of a road map to modify the next-hop attribute.

1. Configure BGP to use the local IP address as the next hop of the route

Table 44-30 Configure BGP to Use the Local IP Address as the Next Hop of the Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to use the local IP address as the next hop when advertising a route to the neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **next-hop-self**	Required By default, the next-hop attribute advertised to the EBGP neighbor is the local IP address and advertised to the IBGP will be maintained and not be changed.

NOTE

- When BGP is configured to use the local IP address as the next hop of the route, if the source address of the TCP session is configured using **neighbor update-source**, the source address will be used as the next-hop address; otherwise, the output interface IP of the advertising device will be selected as the local IP address.

2. Configure a route map to modify the NEXT-HOP attribute

BGP supports the configuration of a route map to modify the NEXT-HOP attribute and the next-hop attribute can be modified through **set ip next-hop**.

Table 44-31 Configure a Route Map to Modify the NEXT-HOP Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a route map to modify the NEXT-HOP attribute	**neighbor** { *neighbor-address* **|** *peer-group-name* } **route-map** *rtmap-name* **in | out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the NEXT-HOP attribute, you need to modify the NEXT-HOP attribute through the command **set ip next-hop**. See PBR Tools - Technical manual - **set ip next-hop**.

Configure BGP Route Community Attributes

BGP supports configuration to send the community attributes when advertising the routes to a neighbor. The route map can be applied on the specified neighbor to match the community attributes in both incoming and outgoing directions.

The community attributes are used to identify a set of routes to apply the route policy on the routes. The community attributes are in two forms, standard and extended. The standard community attribute is 4 bytes long, including NO_EXPORT, LOCAL_AS, NO_ADVERTISE and INTERNET; the extended community attribute is 8 bytes long, including Route Target (RT) and Route Origin.

1. Configure BGP to advertise the route community attributes to neighbors

The **neighbor send-community** supports advertisements of the standard or extended community attributes, or both, to the neighbors.

Table 44-32 Configure BGP to Advertise the Route Community Attributes to Neighbors

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to advertise the route community attributes to neighbors	**neighbor** { *neighbor-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]	Required By default, no community attribute is advertised to any neighbor.

NOTE

- After activating a neighbor under VPNv4 address family, BGP will automatically advertise the standard and extended community attributes to the neighbor.

2. Configure a route map to modify the community attributes

BGP supports the configuration of a route map to modify the community attributes, and the community attributes may be modified through **set communtiy**.

Table 44-33 Configure a Route Map to Modify the Community Attributes

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a route map to modify the community attributes	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in** | **out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the community attributes, you need to modify the community attributes through the command **set communtiy**. See PBR Tools - Technical manual **-set communtiy**.

44.2.5 Configure BGP Network Optimization *-E -A*

Configuration Conditions

Before configuring the BGP network optimization, ensure that:

- Enable BGP;
- Configure a BGP neighbor and establish a session successfully.

Configure BGP Neighbor Keepalive Time

After successful establishment of a BGP session, neighbors will periodically send Keepalive messages to maintain the BGP session relationship. BGP session will be disconnected over time if no Keepalive message or route update is received from the neighbor within the session Holdtime. The session Keepalive time will not exceed one third of the Holdtime.

Table 44-34 Configure Keepalive Time of a BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the global BGP Keepalive time and Holdtime	**timers bgp** *keepalive-interval holdtime-interval*	Optional By default, the Keepalive timer interval is 60s, the hold-down timer interval is 180s and the session reconnection timer interval is 120s.
Configure the Keepalive time and Holdtime of a BGP neighbor or peer group	**neighbor** { *neighbor-address* | *peer-group-name* } **timers** { *keepalive-interval holdtime-interval* | **connect** *connect-interval* }	

NOTE

- The Keepalive time and Holdtime configured for the specified neighbor take precedence over the global BGP Keepalive time and Holdtime.
- After neighbor negotiation, the minimum Holdtime will be used as the Holdtime of the BGP session.
- When both the Keepalive time and Holdtime are configured to zero, the neighbor Keepalive/hold function will be disabled.
- When the Keepalive interval exceeds one third of the Holdtime, BGP will send a Keepalive

packet using one third of the Holdtime.

Configure BGP Route Scan Time

BGP mainly completes the pathfinding process with AS the unit, and IGP completes the internal pathfinding of AS, so BGP route usually relies on IGP route. After the next hop or output interface of the IGP route on which GGP relies changes, BGP updates the BGP route by regularly scanning the IGP route and completes the local BGP route update in the scan cycle.

Table 44-35 Configure BGP Route Scan Time

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP route scan time	**bgp scan-time** *time*	Optional By default, the BGP route scan time is 60s.

NOTE

- Too short BGP route scan time will make BGP frequently scan the route, affecting the device performance.

Configure EBGP Neighbor Fast Failover

After successful establishment of a BGP session, neighbors will periodically send Keepalive messages to each other to maintain the BGP session relationship. BGP session will be disconnected over time if no Keepalive message or route update is received from the neighbor within the session Holdtime. You can configure a direct EBGP neighbor to immediately disconnect the BGP when the connection interface is down without waiting for the BGP Keepalive timeout. When the EBGP neighbor fast failover is canceled, the EBGP session will not respond to the interface down and the BGP session connection will be disconnected through a timeout.

Table 44-36 Configure EBGP Neighbor Fast Failover

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure EBGP neighbor fast failover	**bgp fast-external-failover**	Optional By default, the rapid processing of EBGP in response to direct interface down has been enabled.

Configure BGP Route Suppression

Frequent oscillating routes in the network will cause network instability. BGP can suppress such routes by configuring route dampening to reduce the impact of oscillating routes on the network.

Frequent oscillating routes will be allocated with an increased penalty value. When the penalty value exceeds the suppress limit, the route will not be advertised to the neighbor, and the penalty value cannot exceed the maximum suppression time. When a route does not oscillate during the half-life, the penalty value is halved, and the route is not re-advertised to the neighbor until the value is below the reuse limit.

- Half-life: the time it takes for the route penalty value to be halved.
- Reuse limit: the threshold value used for route recovery.
- Suppress limit: the threshold at which a route is suppressed.
- Maximum suppression time: the maximum time for a route to be suppressed.

Table 44-37 Configure BGP Route Suppression

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the BGP route dampening cycle	**bgp dampening** [*reach-half-life* [*reuse-value suppress-value max-suppress-time* [*unreach-half-life*]] | **route-map** *rtmap-name*]	Required By default, the route suppression is disabled. For the enabled default route, the suppression half-life is 15min, the reuse limit is 750, the suppress limit is 2000, the maximum suppression time is 60min and the unreachable half-life of

		the route penalty is 15min.

NOTE

- The route oscillations include route additions/deletions and route attribute changes, such as next hop and MED attributes.

Configure BGP Neighbor Refresh Capability

When the route policy applied on a BGP neighbor changes, the routing table shall be refreshed again. One method is to restart the session by resetting the BGP connection to reset, which will result in the BGP route oscillation and affect the service operation. The other more graceful method is to configure the local BGP device to support the route refresh capability. When its neighbor needs to reset the route, a Route-Refresh message is advertised to the local device. After receiving the Route-Refresh message, the local device resends the route to the neighbor to achieve dynamic refresh of the routing table without disconnecting the BGP session.

Table 44-38 Configure BGP neighbor refresh capability

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to enable the neighbor refresh capability	**neighbor** { *neighbor-address* | *peer-group-name* } **capability route-refresh**	Optional By default, advertisement to the neighbor to support the route refresh capability has been enabled.

Configure BGP Neighbor Soft-reconfiguration Capability

When the route policy applied on a BGP neighbor changes, the routing table shall be refreshed again. One method is to restart the session by resetting the BGP connection to reset, which will result in the BGP route oscillation and affect the service operation. Another more graceful method is to configure the local BGP device to support the route refresh capability. Another method is to enable the soft-reconfiguration capability of the local BGP device. By default, the BGP device keeps the route information of all neighbors. After enabling the soft-reconfiguration capability of the neighbors, it will refresh the routes of the neighbors kept locally without disconnecting BGP session.

Table 44-39 Configure BGP Neighbor Soft-reconfiguration Capability

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to enable the neighbor soft-reconfiguration capability	**neighbor** { *neighbor-address* | *peer-group-name* } **soft-reconfiguration inbound**	Required By default, the neighbor soft-reconfiguration is disabled.

Configure BGP Neighbor ORF Capability

BGP implements precise route control through rich route attributes, which is usually achieved by applying routing policies in both incoming and outgoing directions and is the behavior of the BGP locally. BGP also supports ORF (Outbound Route Filtering) capability. Through the Route-refresh packet, it advertises the local entry policy to the neighbors and the neighbors advertise the application of the policy to BGP, so as to greatly reduce the interaction of the route update packets between the BGP neighbors.

Successful ORF capability negotiation requires the following:

- Both neighbors need to enable the ORF capability;
- ORF send and ORF receive must be paired. That, if one neighbor is ORF send, the other must be ORF both or ORF receive; if one is ORF receive, the other must be ORF send or ORF both;
- The neighbor using ORF send needs to apply the prefix-list in the incoming direction.

Table 44-40 Configure BGP Neighbor ORF Capability

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a neighbor to apply prefix-list in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **prefix-list** *prefix-list-name* **in**	Required By default, no prefix-list is applied on any BGP neighbor.

Steps	Command	Description
Configure a neighbor to support ORF	**neighbor** { *neighbor-address* | *peer-group-name* } **capability orf prefix-list** { **both** | **receive** | **send** }	Required By default, no neighbor advertisement to support ORF is enabled.

44.2.6 Configure BGP Large Network *-E -A*

Configuration Conditions

Before configuring BGP large network, ensure that:

- Enable BGP;
- Configure a BGP neighbor and establish a session successfully.

Configure BGP Peer Group

A BGP peer group is a collection of BGP neighbors with the same configuration policy, and any configuration for a peer group will affect all peer members at the same time. Configuring the BGP peer group facilitates centralized management and maintenance of neighbors.

Table 44-41 Configure a BGP Peer Group

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Create a BGP peer group	**neighbor** *peer-group-name* **peer-group**	Required By default, no peer group is configured and the neighbors do not join any peer group.
Configure a neighbor to join a peer group	**neighbor** *neighbor-address* **peer-group** *peer-group-name*	

NOTE

- The configuration of a peer group affects all peer group members simultaneously.
- The same configuration as the peer group will be deleted when a neighbor joins the peer group.

- When a route policy is configured for the outgoing or incoming direction of a peer group, after the route policy changes, it will not be effective for the neighbors that have joined the peer group. The changed route policy can be effective for the peer group members only after the peer group is re-configured.

Configure BGP Route Reflector

In a large BGP networking environment, the whole network connection of IBGP neighbors is required, that is, each BGP establishes connection with all other IBGP neighbors, so the number of BGP connections in the networking environment of N BGP neighbors is N*(n-1)/2. The greater the number of connections, the greater the number of route advertisements. The BGP route reflector is a way to reduce the number of network connections. It divides several IBGPs into a group and specifies a BGP as the reflector (RR), the other BGPs as the clients, and the BGP in the non-group as the non-client. The client only peers with RR and not with other BGPs, thereby reducing the number of necessary IBGP connections to N-1.

Route reflection principle of BGP route reflector:

- Routes learnt from non-client IBGP neighbors are reflected to clients only;
- Routes learnt from clients are reflected to all clients and non-clients except the client that initiates the route;
- Routes learnt from the neighbors are reflected to all clients and non-clients.

Table 44-42 Configure BGP Route Reflector

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a reflector cluster ID	**bgp cluster-id** { *cluster-id-in-ip* | *cluster-id-in-num* }	Required By default, the device Router ID is used as the reflector cluster ID.
Configure a neighbor as the reflector client	**neighbor** { *neighbor-address* | *peer-group-name* } **route-reflector-client**	Required By default, no neighbor is specified as the reflector client.
Configure the BGP client-to-client reflection	**bgp client-to-client reflection**	Optional By default, the BGP route client-to-client reflection has been enabled.

NOTE

- The reflector cluster ID is used to identify the same reflector area in which multiple reflectors may exist and have the same reflector cluster ID.

Configure BGP Confederation

In a large BGP networking environment, the whole network connection of IBGP neighbors is required, that is, each BGP establishes connection with all other IBGP neighbors, so the number of BGP connections in the networking environment of N BGP neighbors is N*(n-1)/2. The greater the number of connections, the greater the number of route advertisements. BGP confederation is another method to reduce the number of network connections. With the divide-and-rule policy, it divides an AS into several sub-AS areas. Each AS area form a confederation. The confederations are fully connected through IBGP. The sub-AS areas in a confederation are connected by EBGP, effectively reducing the number of BGP connections.

When configuring a BGP confederation, you need to assign a confederation ID to each confederation and specify its members. The confederation is different from the route reflector. Under the route reflector conditions, only the route reflector is required to support the route reflection, while the confederation requires all members to support the confederation function.

Table 44-43 Configure BGP confederation

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Create the BGP confederation ID	**bgp confederation identifier** *as-number*	Required By default, no confederation AS number is configured.
Configure a confederation member	**bgp confederation peers** *as-number-list*	Required By default, no confederation sub-AS number is configured.

NOTE

- The confederation ID is used to identify the confederation sub-AS and the confederation

members are distributed to the sub-AS.

44.2.7 Configure BGP GR *-E -A*

GR (Graceful Restart) is used to keep the route information at the forwarding level of the local device and neighbor device unchanged and the forwarding not affected during the master-backup switching; after the device switching and re-running, the two devices synchronize the route information at the protocol level and update the forward layer, so as to achieve the purpose of uninterrupted data forwarding during the switching process.

Roles in GR process:

- GR Restarter: a device that performs protocol GR;
- GR Helper: a device that helps the protocol GR;
- GR Time: maximum restart time of GR-Restarter. The GR Helper only keeps the route stable for that time.

Dual-master control devices can serve as GR Restarter and GR Helper, while centralized devices can only serve as GR Helper to assist the Restarter end to complete GR. When GR Restarter performs GR, the GR Helper maintains its route until the GR Time expires. After assisting the GR Restarter in completing GR, the GR Helper synchronizes the route message. In this period, the network route and packet forwarding remain in the state before GR, effectively guaranteeing the network stability.

The BGP GR relationship is established by OPEN packet negotiation when neighbors are connected. When the GR Restarter neighbor restarts, the BGP session is disconnected, but the routes learnt from that neighbor are not deleted and are still forwarded normally in the IP routing table. These routes are only marked Stale in the BGP routing table and will be updated after GR completion or timeout.

GR Restarter needs to complete the connection with the GR Helper within the maximum allowed time, otherwise, the GR Helper will remove the remaining GR routes and remove the GR process. After the neighbor reconnection, the GR Helper needs to receive the update packet with End-Of-RIB tag from the GR Restarter to complete the GR process successfully; otherwise, the GR routes not updated will be deleted after the maximum Holdtime (stalepath-time) and the GR relationship will be canceled.

Configuration Conditions

Before configuring the BGP GR, ensure that:

- Enable BGP;
- Configure a BGP neighbor and establish a session successfully.

Configure BGP GR Restarter

Table 44-44 Configure BGP GR Restarter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enable the BGP GR capability	**bgp graceful-restart** [**restart-time** *time* | **stalepath-time** *time*]	Required By default, the GR capability of the BGP device is disabled. The maximum allowed time for the session re-establishment of the default neighbors with enabled GR is 120s and the maximum Holdtime of the GR route is 360s.
Configure advertisement of the GR-Restarter capability to the neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **capability graceful-restart**	Required By default, the GR Restarter capability is not advertised to the neighbor.

Configure BGP GR Helper

Table 44-45 Configure BGP GR Helper

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enable the BGP GR capability	**bgp graceful-restart** [**restart-time** *time* | **stalepath-time** *time*]	Required By default, the GR capability of the BGP device is disabled. The maximum allowed time for the session re-establishment of the default neighbors with enabled GR is 120s and the maximum Holdtime of the GR route is 360s.

44.2.8 Configure BGP to Link with BFD -E -A

In general, there are other intermediate devices running between BGP neighbors. When these intermediate devices fail, the BGP session is still normal in Holdtime and cannot respond to the link failure of intermediate devices in a timely manner. BFD provides a method for quickly detecting the state of the line between two devices. When BFD detection is enabled between the BGP devices, if there is a line fault between the devices, BFD will quickly detect the line fault, notify BGP, trigger BGP to quickly disconnect the session and switch to the backup line to achieve quick route switching.

Configuration Conditions

Before configuring BGP to link with BFD, ensure that:

- Enable BGP;
- Configure a BGP neighbor and establish a session successfully.

Configure EBGP to Link with BFD

EBGP coordination with BFD is based on the single-hop BFD session. The BFD session parameters shall be configured in the interface mode.

Table 44-46 Configure EBGP to Link with BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure EBGP to link with BFD	**neighbor** { *neighbor-address* | *peer-group-name* } **fall-over bfd**	Required By default, the neighbor BFD is disabled
Exit the BGP configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the minimum receive interval of BFD session	**bfd min-receive-interval** *milliseconds*	Optional By default, the minimum receive interval of BFD session is 1000s

Steps	Command	Description
Configure the minimum send interval of BFD session	**bfd min-transmit-interval** *milliseconds*	Optional By default, the minimum send interval of BFD session is 1000s
Configure BFD session detection timeout multiplier	**bfd multiplier** *number*	Optional By default, the BFD session detection timeout multiplier is 5

NOTE

- Refer to the Reliability technology - BFD technical manual and BFD configuration manual for relevant BFD configuration.

44.2.9 BGP Monitoring and Maintaining -E -A

Table 44-47 BGP Monitoring and Maintaining

Command	Description
clear ip bgp { ***** | *neighbor-address* | *as-number* | **peer-group** *peer-group-name* | **external** } [**vrf** *vrf-name* | **ipv4 unicast** | **ipv4 multicast** | **vpnv4 unicast** | **mvpn**]	Reset the BGP neighbor
clear ip bgp [**ipv4 unicast** | **ipv4 multicast**] **dampening** [*ip-address* | *ip-address/mask-length*]	Clear the dampening route
clear ip bgp [**ipv4 unicast** | **ipv4 multicast**] **flap-statistics** [*ip-address* | *ip-address/mask-length*]	Clear the flap statistics
clear ip bgp { ***** | *neighbor-address* | *as-number* | **peer-group** *peer-group-name* | **external** } [**ipv4 unicast** | **ipv4 multicast** | **vpnv4 unicast** | **vrf**	Soft-reconfigure the neighbor

Command	Description
vrf-name | mvpn] { [**soft**] [**in** | **out**] }	
clear ip bgp { ***** | *neighbor-address* } **in** { **ecomm** | **prefix-filter** }	Advertise ORF to the neighbor
show ip bgp [**vpnv4** { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* }] [*ip-address* | *ip-address*/*mask-length*]	Show the route information under the corresponding address family of BGP
show ip bgp attribute-info	Show the information about public route attributes of BGP
show ip bgp cidr-only	Show all classful network routes of BGP
show ip bgp community [*community-number* / *aa:nn* / **exact-match** / **local-AS** / **no-advertise** / **no-export**]	Show the route information that matches the specified community attributes
show ip bgp community-info	Show all community attribute information of BGP
show ip bgp community-list *community-list-name*	Show the Community list where the route information is applied
show ip bgp [**vpnv4** { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* }] **dampening** { **dampened-paths** | **flap-statistics** | **parameters** }	Show the detailed information of route dampening
show ip bgp filter-list *filter-list-name* [**exact-match**]	Show the routes that the AS_PATH ACL matches
show ip bgp inconsistent-a	Show conflicting routes of AS_PATH
show ip bgp ipv4 vpn-target [*vpn-rt*]	Show VPN-TARGET routing table of BGP
show ip bgp ipv4 vpn-target rt-filter [**neighbor** *ip-address*]	Show RT filtering table of BGP neighbors
show ip bgp mvpn { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } { **all-type** | **type** { **1** [*ip-address*] |	Show the route information under BGP MVPN address family

Command	Description
7[*as:source-ip-address:group-ip-address*] } }	
show ip bgp mvpn { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } { **neighbors** *ip-address* } { **advertised-routes** | **received-routes** | **routes** } { **all-type** | **type** { **1** [*ip-address*] | **7** [*as:source-ip-address:group-ip-address*] } }	Show the route information of specified neighbors under BGP MVPN family address
show ip bgp mvpn {**all** | **vrf** *vrf-name* | **rd** *route-distinguisher* | **neighbors** *ip-address* } { **all-type** | **type** { **1** | **7** } } { **statistics** }	Show the route statistics under BGP MVPN family address
show ip bgp [**vpnv4** { **all** | **vrf** *vrf_name* **|** **rd** *route-distinguisher* }] **neighbors** [*ip-address*]	Show the detailed information about BGP neighbors
show ip bgp orf ecomm	Show ORF information of all BGP neighbors
show ip bgp paths	Show AS_PATH information of BGP route
show ip bgp prefix-list *prefix-list-name*	Show the routes that the prefix-list matches
show ip bgp quote-regexp *as-path-list-name*	Show the routes that the AS_PATH list matches
show ip bgp regexp *as-path-list-name*	Show the routes that the AS_PATH list matches
show ip bgp route-map *rtmap-name*	Show the routing that the route map matches
show ip bgp scan	Show BGP scan information
show ip bgp [**vpnv4** { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } | **mvpn**] **summary**	Show the information about the neighbor summary of BGP

44.2.10 BGP Monitoring and Maintaining -E -A

Table 44-48 BGP Monitoring and Maintaining

Command	Description
clear ip bgp { * [**vrf** *vrf-name*] **|** *neighbor-address* [**vrf** *vrf-name*] **|** *as-number* **| peer-group** *peer-group-name* **| external** }	Reset the BGP neighbor
clear ip bgp [**ipv4 unicast | ipv4 multicast**] **dampening** [*ip-address* | *ip-address*/*mask-length*]	Clear the dampening route
clear ip bgp [**ipv4 unicast | ipv4 multicast**] **flap-statistics** [*ip-address* | *ip-address*/*mask-length*]	Clear the flap statistics
clear ip bgp { * | *neighbor-address* | *as-number* **| peer-group** *peer-group-name* **| external** } [**ipv4 unicast | ipv4 multicast | vpnv4 unicast | vrf** *vrf-name*] { [**soft**] [**in | out**] }	Soft-reconfigure the neighbor
clear ip bgp { * | *neighbor-address* } **in** { **ecomm | prefix-filter** }	Advertise ORF to the neighbor
show ip bgp [**vpnv4** { **all | vrf** *vrf-name* | **rd** *route-distinguisher* }] [*ip-address* | *ip-address*/*mask-length*]	Show the route information under the corresponding address family of BGP
show ip bgp attribute-info	Show the information about public route attributes of BGP
show ip bgp cidr-only	Show all classful network routes of BGP
show ip bgp community [*community-number* / *aa:nn* / **exact-match** / **local-AS** / **no-advertise** / **no-export**]	Show the route information that matches the specified community attributes
show ip bgp community-info	Show all community attribute information of BGP
show ip bgp community-list *community-list-name*	Show the Community list where the route information is applied

Command	Description
show ip bgp [**vpnv4** { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* }] **dampening** { **dampened-paths** | **flap-statistics** | **parameters** }	Show the detailed information of route dampening
show ip bgp filter-list *filter-list-name* [**exact-match**]	Show the routes that the AS_PATH ACL matches
show ip bgp inconsistent-as	Show conflicting routes of AS_PATH
show ip bgp [**vpnv4 all**] **neighbors** [*ip-address*]	Show the detailed information about BGP neighbors
show ip bgp orf ecomm	Show ORF information of all BGP neighbors
show ip bgp paths	Show AS_PATH information of BGP route
show ip bgp prefix-list *prefix-list-name*	Show the routes that the prefix-list matches
show ip bgp quote-regexp *as-path-list-name*	Show the routes that the AS_PATH list matches
show ip bgp regexp *as-path-list-name*	Show the routes that the AS_PATH list matches
show ip bgp route-map *rtmap-name*	Show the routing that the route map matches
show ip bgp scan	Show BGP scan information
show ip bgp [**vpnv4** { **all** | **vrf** *vrf-name* | **rd** *route-distinguisher* } | vxlan] **summary**	Show the information about the neighbor summary of BGP
show ip bgp vxlan local-remote [*ip-address* | **neighbor** *ip-address*]	Show the local Session information advertised by BGP to the neighbor
show ip bgp vxlan session [*ip-address* | **active**]	Show the Session information learnt by BGP

44.3 BGP Typical Configuration Example

44.3.1 Configure Basic Functions of BGP

-E -A

Network Requirements

- Establish EBGP neighbors between Device1 and Device2 and IBGP neighbors between Device2 and Device3.
- Device1 learns the interface direct route 200.0.0.0/24 from Device3, and Device3 learns the interface direct route 100.0.0.0/24 from Device1.

Network Topology

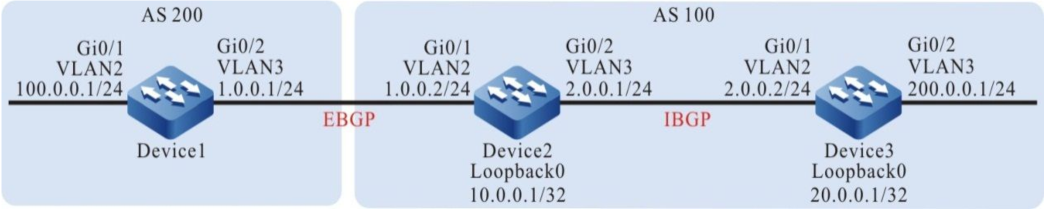


Figure 44-1 Networking for Configuring the Basic Functions of BGP

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF to make the Loopback routes between the devices are mutually reachable.

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


O   20.0.0.1/32 [110/2] via 2.0.0.2, 12:27:09 AM, vlan3
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


O   10.0.0.1/32 [110/2] via 2.0.0.1, 12:28:13 AM, vlan2
```

As you can see, Device2 and Device3 have learned the peer Loopback routes by running the OSPF protocol to prepare for establishing IBGP neighbors through the Loopback in the next step.

Step 4:   Configure BGP.

#Configure Device1.

Configure an EBGP peer that establishes direct connection with Device2 and introduce 100.0.0.0/24 to BGP through network.

```
Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 100
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#Configure Device2.

Configure an IBGP peer that establishes non-direct connection with Device3 through Loopback0, set the next hop of the advertisement route to itself and configure an EBGP peer that establishes direct connection with Device1.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 200
Device2(config-bgp)#neighbor 20.0.0.1 next-hop-self
Device2(config-bgp)#exit
```

#Configure Device3.

Establish non-direct IBGP peer relationship with Device2 through Loopback0 and introduce 200.0.0.0/24 to BGP through network.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 remote-as 100
```

```
Device3(config-bgp)#neighbor 10.0.0.1 update-source loopback0

Device3(config-bgp)#network 200.0.0.0 255.255.255.0

Device3(config-bgp)#exit
```

NOTE

- To prevent route oscillations, all IBGP neighbors are established through the Loopbacks, and OSPF is required to synchronize the route information of the Loopbacks between IBGP neighbors.

Step 5: Check the result.

#Query the BGP neighbor state on Device2.

```
Device2#show ip bgp summary

BGP router identifier 10.0.0.1, local AS number 100

BGP table version is 2

2 BGP AS-PATH entries

0 BGP community entries


Neighbor        V    AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down  State/PfxRcd

1.0.0.1         4   200       3       3        1    0    0 00:00:29        1

20.0.0.1        4   100       5       4        2    0    0 00:02:13        1
```

It can be seen from the numbers (number of prefixes of routes received from the neighbors) in the column State/PfxRcd that Device2 has successfully established BGP neighbors with Device1 and Device3.

#Query the routing table of Device1.

```
Device1#show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management

       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


B   200.0.0.0/24 [20/0] via 1.0.0.2, 00:15:52, vlan3
```

#Query the routing table of Device2.

```
Device2#show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management

       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set
```

```
B   100.0.0.0/24 [20/0] via 1.0.0.1, 12:14:11 AM, vlan2
B   200.0.0.0/24 [200/0] via 20.0.0.1, 12:17:12 AM, vlan3
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   100.0.0.0/24 [200/0] via 10.0.0.1, 12:14:50 AM, vlan2
```

As you can see, Device1 learns the interface direct route 200.0.0.0/24 from Device3, and Device3 learns the interface direct route 100.0.0.0/24 from Device1.

44.3.2 Configure BGP Route Re-distribution -E -A

Network Requirements

- Establish an OSPF neighbor between Device3 and Device2 and advertise the interface direct route 200.0.0.0/24 to Device2.
- Establish EBGP neighbors between Device1 and Device2. Device2 Re-distributes the learned OSPF route to BGP and advertises to Device1.

Network Topology

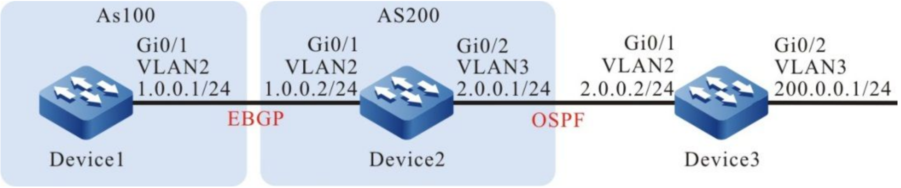


Figure 44-2 Networking for Configuring BGP to Re-distribute Routes

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF to make the Loopback routes between the devices are mutually reachable.

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device2.

```
Device2#show ip route ospf
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   200.0.0.0/24 [110/2] via 2.0.0.2, 12:01:45 AM, vlan3
```

According to the routing table, Device2 has learned the OSPF route 200.0.0.0/24 advertised by Device3.

Step 4: Configure BGP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 100
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 200
Device2(config-bgp)#exit
```

#Query the BGP neighbor state on Device2.

```
Device2#show ip bgp summary
BGP router identifier 2.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.0.0.1         4   200       2       2        2    0    0 12:00:42 AM        0
```

As you can see, Device2 has successfully established a BGP neighbor with Device1.

Step 5: Configure BGP to Re-distribute OSPF routes.

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#redistribute ospf 100
Device2(config-bgp)#exit
```

Step 6: Check the result.

#Query the BGP routing table of Device2.

```
Device2#show ip bgp
BGP table version is 6, local router ID is 2.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
[O]*> 2.0.0.0/24        0.0.0.0              1        32768 ?
[O]*> 200.0.0.0/24       2.0.0.2              2        32768 ?
```

As you can see, the OSPF routes have been successfully Re-distributed to BGP.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   2.0.0.0/24 [20/1] via 1.0.0.2, 12:06:14 AM, vlan2
B   200.0.0.0/24 [20/2] via 1.0.0.2, 12:06:14 AM, vlan2
```

As you can see, Device1 has successfully learned the routes 2.0.0.0/24 and 200.0.0.0/24.

NOTE

- In an actual application, if there are two or more AS boundary routers, it is recommended that you do not Re-distribute routes between different routing protocols. If route Re-distribution must be configured, you are required to configure route control policies such as route filtration and filtration summary on the AS boundary routers to prevent routing loops.

44.3.3 Configure BGP Community Attributes -E -A

Network Requirements

- Establish EBGP neighbors between Device1 and Device2.
- Device1 introduces two direct routes 100.0.0.0/24 and 200.0.0.0/24 to BGP through network and sets different community attributes to two routes when advertising to Device2.
- When receiving the routes advertised by Device1, Device2 filters the route 100.0.0.0/24 and allows the route 200.0.0.0/24 by matching the community attributes in the incoming direction of the neighbor.

Network Topology

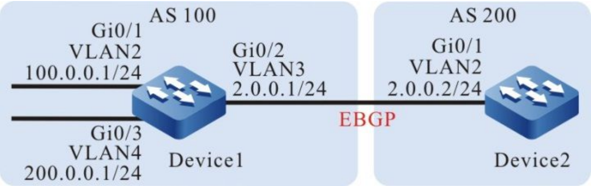


Figure 44-3 Networking for Configuring BGP Community Attributes

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure BGP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 2.0.0.2 remote-as 200
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#network 200.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 2.0.0.1 remote-as 100
Device2(config-bgp)#exit
```

#Query the BGP neighbor state on Device1.

```
Device1#show ip bgp summary
BGP router identifier 200.0.0.1, local AS number 100
BGP table version is 1
```

```
1 BGP AS-PATH entries
0 BGP community entries


Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.0.0.2         4   200       2       3        1    0    0 12:00:04 AM        0
```

As you can see, Device1 has successfully established a BGP neighbor with Device2.

#Query the routing table on Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


B   100.0.0.0/24 [20/0] via 2.0.0.1, 12:07:47 AM, vlan2
B   200.0.0.0/24 [20/0] via 2.0.0.1, 12:07:47 AM, vlan2
```

As you can see, Device2 has successfully learned the routes 100.0.0.0/24 and 200.0.0.0/24.

Step 4: Configure an ACL and route policy and set BGP community attributes.

#Configure Device1.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#ip access-list standard 2
Device1(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#route-map CommunitySet 10
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set community 100:1
Device1(config-route-map)#exit
Device1(config)#route-map CommunitySet 20
Device1(config-route-map)#match ip address 2
Device1(config-route-map)#set community 100:2
Device1(config-route-map)#exit
```

Set different community attributes to the routes 100.0.0.0/24 and 200.0.0.0/24 by configuring an ACL and route policy.

Step 5: Configure route policy for BGP.

#Configure Device1.

```
Device1(config)#router bgp 100
```

```
Device1(config-bgp)#neighbor 2.0.0.2 route-map CommunitySet out
Device1(config-bgp)#neighbor 2.0.0.2 send-community
Device1(config-bgp)#exit
```

#Query the BGP routing table of Device2.

```
Device2#show ip bgp 100.0.0.0
BGP routing table entry for 100.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  100
    2.0.0.1 (metric 10) from 2.0.0.1 (10.0.0.1)

      Origin IGP, metric 0, localpref 100, valid, external, best
       Community: 100:1
       Last update: 00:01:06 ago

Device2#show ip bgp 200.0.0.0
BGP routing table entry for 200.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  100
    2.0.0.1 (metric 10) from 2.0.0.1 (10.0.0.1)

      Origin IGP, metric 0, localpref 100, valid, external, best
       Community: 100:2
       Last update: 12:01:10 AM ago
```

According to BGP routing table of Device2, the community attribute of the route 100.0.0.0/24 is set to 100:1 and of 200.0.0.0/24 is set to 100: 2.

Step 6: Configure BGP route filtration.

#Configure Device2.

```
Device2(config)#ip community-list 1 permit 100:2
Device2(config)#route-map communityfilter
Device2(config-route-map)#match community 1
Device2(config-route-map)#exit
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 2.0.0.1 route-map communityfilter in
Device2(config-bgp)#exit
```

Step 7: Check the result.

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   200.0.0.0/24 [20/0] via 2.0.0.1, 12:00:53 AM, vlan2
```

According to BGP routing table of Device2, the route 100.0.0.0/24 is filtered in the incoming direction and the route 200.0.0.0/24 is allowed.

NOTE

- The route policy configured on the peer may take effect only after BGP process is re-configured.
- The community attributes can be advertised to the peer only after the command send-community is configured.

44.3.4 Configure BGP Route Reflector *-E -A*

Network Requirements

- Establish EBGP neighbors between Device3 and Device4. Device4 advertises the route 100.0.0.0/24 to Device3.
- Device2 establishes IBGP neighbors with Device3 and Device1 respectively. Configure a route reflector on Device2, with Device1 and Device3 as the clients, so that Device1 can learn the route 100.0.0.0/24 advertised by Device4.

Network Topology

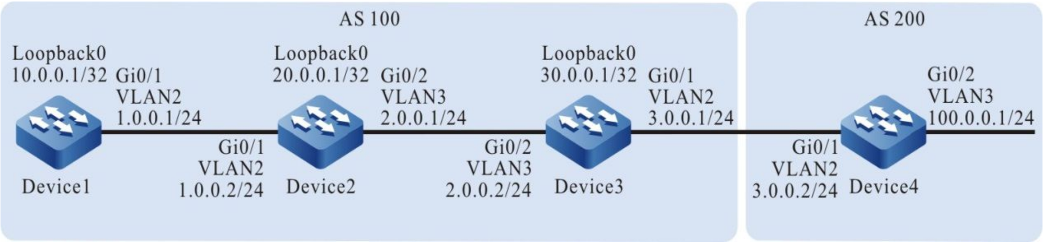


Figure 44-4 Networking for Configuring BGP Route Reflector

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF to make the Loopback routes between the devices are mutually reachable.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device2#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   2.0.0.0/24 [110/2] via 1.0.0.2, 1:12:00 AM, vlan2
O   20.0.0.1/32 [110/2] via 1.0.0.2, 1:11:47 AM, vlan2
O   30.0.0.1/32 [110/3] via 1.0.0.2, 1:07:47 AM, vlan2
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

```
O   10.0.0.1/32 [110/2] via 1.0.0.1, 1:13:02 AM, vlan2
O   30.0.0.1/32 [110/2] via 2.0.0.2, 1:08:58 AM, vlan3
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   1.0.0.0/24 [110/2] via 2.0.0.1, 1:10:04 AM, vlan2
O   10.0.0.1/32 [110/3] via 2.0.0.1, 1:10:04 AM, vlan2
O   20.0.0.1/32 [110/2] via 2.0.0.1, 1:10:04 AM, vlan2
```

As you can see, Device1, Device2 and Device3 learn each other's loopback routes.

Step 4: Configure BGP.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 3.0.0.2 remote-as 200
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#neighbor 20.0.0.1 next-hop-self
Device3(config-bgp)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#neighbor 3.0.0.1 remote-as 100
Device4(config-bgp)#network 100.0.0.0 255.255.255.0
```

```
Device4(config-bgp)#exit
```

#Query the BGP neighbor state on Device2.

```
Device2#show ip bgp summary
BGP router identifier 20.0.0.1, local AS number 100
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.1        4   100       8       8        1    0    0 12:03:01 AM        0
30.0.0.1        4   100       9       9        1    0    0 12:02:41 AM        1
```

#Query the BGP neighbor state on Device4.

```
Device4#show ip bgp summary
BGP router identifier 100.0.0.1, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.0.0.1         4   100      19      19        1    0    0 00:05:40        0
```

As you can see, BGP neighbors are established successfully between the devices.

#Query the BGP routing table of Device3.

```
Device3#show ip bgp
BGP table version is 2, local router ID is 30.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network           Next Hop          Metric LocPrf Weight Path
[B]*> 100.0.0.0/24       3.0.0.2              0            0 200 i
```

#Query the BGP routing table of Device2.

```
Device2#show ip bgp
BGP table version is 768, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network           Next Hop          Metric LocPrf Weight Path
[B]*>i100.0.0.0/24       30.0.0.1             0    100      0 200 i
```

#Query the BGP routing table of Device1.

```
Device1#show ip bgp
```

```
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop          Metric LocPrf Weight Path
```

According to the above results, Device2 and Device3 have learned the route 100.0.0.0/24, while Device2 does not advertise the route to Device1.

Step 5: Configure BGP route reflector.

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 route-reflector-client
Device2(config-bgp)#neighbor                          30.0.0.1                          route-reflector-client
Device2(config-bgp)#exit
```

On Device2, configure Device1 and Device3 as the clients of the route reflector.

Step 6: Check the result.

#Query the routing table of Device1.

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop          Metric LocPrf Weight Path
[B]*>i100.0.0.0/24       30.0.0.1              0    100      0 200 i

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
     D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   100.0.0.0/24 [200/0] via 30.0.0.1, 12:01:40 AM, vlan2
```

In BGP of Device2, configure Device1 and Device3 as the clients of the route reflector. Device2 successfully reflects the route 100.0.0.0/24 to the client Device1.

NOTE

- When a peer is configured as the client of the route reflector, the device and the neighbor of that peer are re-configured.

44.3.5 Configure BGP Route Aggregation -E -A

Network Requirements

- Establish an OSPF neighbor between Device1 and Device3. Device3 advertises two routes 100.1.0.0/24 and 100.2.0.0/24 to Device1.
- Establish EBGP neighbors between Device1 and Device2.
- On Device1, aggregate 100.1.0.0/24 and 100.2.0.0/24 into the route 100.0.0.0/14 and advertise to Device2.

Network Topology

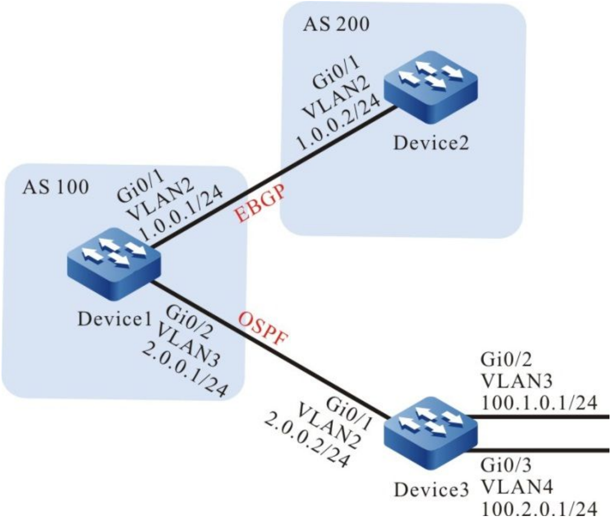


Figure 44-5 Networking for Configuring BGP Route Aggregation

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF to make the Loopback routes between the devices are mutually reachable.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 100.1.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 100.2.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   100.1.0.0/24 [110/2] via 2.0.0.2, 12:00:24 AM, vlan3
O   100.2.0.0/24 [110/2] via 2.0.0.2, 12:00:24 AM, vlan3
```

As you can see, Device1 has learned the routes 100.1.0.0/24 and 100.2.0.0/24 advertised by Device3.

Step 4: Configure BGP.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#exit
```

#Query the BGP neighbor state on Device1.

```
Device1#show ip bgp summary
BGP router identifier 1.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.0.0.2         4   200       2       2        2    0    0 12:00:42 AM        0
```

Device1 has successfully established a BGP neighbor with Device2.

Step 5: Configure BGP route aggregation.

Here are two solutions to fulfill the network needs:

Solution 1: configure an aggregate static route to null0 and introduce it to BGP.

#Configure Device1.

```
Device1(config)#ip route 100.0.0.0 255.252.0.0 null0

Device1(config)#router bgp 100

Device1(config-bgp)#network 100.0.0.0 255.252.0.0

Device1(config-bgp)#exit
```

Check the result.

#Query the BGP routing table of Device1.

```
Device1#show ip bgp

BGP table version is 2, local router ID is 10.0.0.1

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

        S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path

[B]*> 100.0.0.0/14       0.0.0.0                         32768 i
```

As you can see, the aggregate route 100.0.0.0/14 has been generated in the BGP routing table of Device1.

#Query the routing table of Device2.

```
Device2#show ip bgp

BGP table version is 3, local router ID is 20.0.0.1

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

        S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path

[B]*> 100.0.0.0/14       1.0.0.1              0           0 100 i


Device2#show ip route

Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management

    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


B   100.0.0.0/14 [20/0] via 1.0.0.1, 1:39:30 AM, vlan2
```

As you can see, Device2 has successfully learned the aggregate route 100.0.0.0/14 advertised by Device1.

Solution 2: introduce the detailed routes to BGP and then aggregate the routes through the command **aggregate-address**.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#redistribute ospf 100
Device1(config-bgp)#aggregate-address 100.0.0.0 255.252.0.0 summary-only
Device1(config-bgp)#exit
```

Check the result.

#Query the BGP routing table of Device1.

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
[B]*> 100.0.0.0/14       0.0.0.0                    32768 i
[B]s> 100.1.0.0/24       2.0.0.2              2       32768 i
[B]s> 100.2.0.0/24       2.0.0.2              2       32768 i
```

As you can see, the aggregate route 100.0.0.0/14 has been generated in the BGP routing table of Device1.

#Query the routing table of Device2.

```
Device2#show ip bgp
BGP table version is 3, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
[B]*> 100.0.0.0/14       1.0.0.1              0           0 100 i


Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


B   100.0.0.0/14 [20/0] via 1.0.0.1, 1:39:30 AM, vlan2
```

As you can see, Device2 has successfully learned the aggregate route 100.0.0.0/14 advertised by Device1.

NOTE

- In using the aggregate-address command for route aggregation, if you configure the extended command summary-only, the device will only advertise the aggregate route; otherwise, it will advertise the detailed routes and aggregate route simultaneously.

44.3.6 Configure BGP Route Preference

-E -A

Network Requirements

- Device1 establishes IBGP neighbors with Device2 and Device3 respectively and Device4 establishes EBGP neighbors with Device2 and Device3 respectively.
- Device1 advertises two routes 55.0.0.0/24 and 65.0.0.0/24 to Device4; Device4 advertises two routes 75.0.0.0/24 and 85.0.0.0/24 to Device1.
- By modifying the Local-preference attribute of the routes on Device2 and Device3, Device1 prefers the route 75.0.0.0/24 advertised by Device2 and the route 85.0.0.0/24 advertised by Device3.
- By modifying the MED attribute of the routes on Device2 and Device3, Device4 prefers the route 55.0.0.0/24 advertised by Device2 and the route 65.0.0.0/24 advertised by Device3.

Network Topology

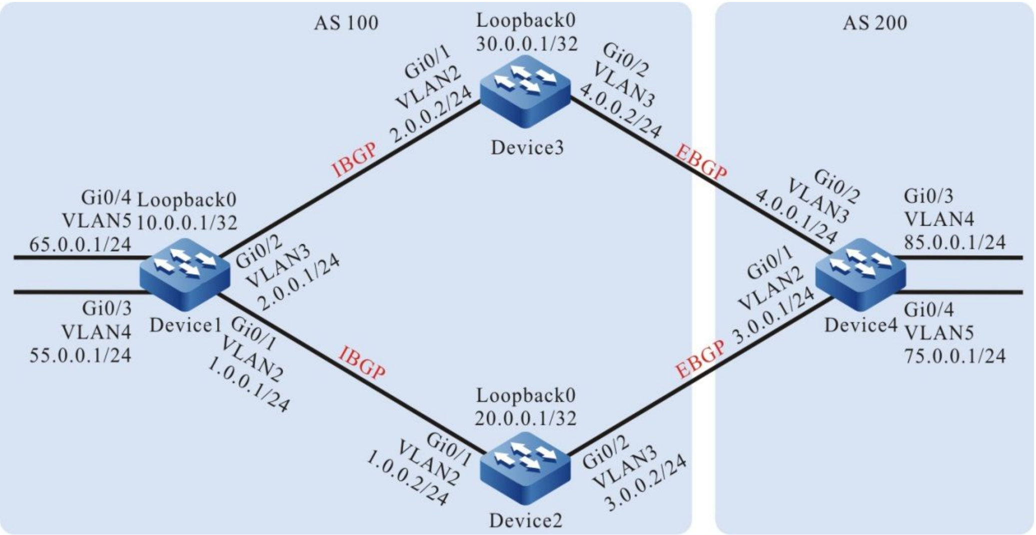


Figure 44-6 Networking for Configuring BGP Route Preference

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF to make the Loopback routes between the devices are mutually reachable.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   20.0.0.1/32 [110/2] via 1.0.0.2, 12:03:15 AM, vlan2
O   30.0.0.1/32 [110/2] via 2.0.0.2, 12:01:40 AM, vlan3
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   2.0.0.0/24 [110/2] via 1.0.0.1, 12:03:54 AM, vlan2
O   10.0.0.1/32 [110/2] via 1.0.0.1, 12:03:54 AM, vlan2
O   30.0.0.1/32 [110/3] via 1.0.0.1, 12:02:14 AM, vlan2
```

#Query the routing table of Device3.

```
Device3#show ip route
```

```
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   1.0.0.0/24 [110/2] via 2.0.0.1, 12:02:35 AM, vlan2
O   10.0.0.1/32 [110/2] via 2.0.0.1, 12:02:35 AM, vlan2
O   20.0.0.1/32 [110/3] via 2.0.0.1, 12:02:35 AM, vlan2
```

As you can see, Device1, Device2 and Device3 learn each other's loopback routes.

Step 4: Configure BGP.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device1(config-bgp)#neighbor 30.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device1(config-bgp)#network 55.0.0.0 255.255.255.0
Device1(config-bgp)#network 65.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 10.0.0.1 next-hop-self
Device2(config-bgp)#neighbor 3.0.0.1 remote-as 200
Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device3(config-bgp)#neighbor 10.0.0.1 next-hop-self
Device3(config-bgp)#neighbor 4.0.0.1 remote-as 200
Device3(config-bgp)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#neighbor 3.0.0.2 remote-as 100
Device4(config-bgp)#neighbor 4.0.0.2 remote-as 100
```

```
Device4(config-bgp)#network 75.0.0.0 255.255.255.0
Device4(config-bgp)#network 85.0.0.0 255.255.255.0
Device4(config-bgp)#exit
```

#Query the BGP neighbor state on Device1.

```
Device1#show ip bgp summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor       V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
20.0.0.1       4   100      11      11        2    0    0 00:07:40        2
30.0.0.1       4   100       7       7        2    0    0 12:03:59 AM        2
```

#Query the BGP neighbor state on Device4.

```
Device4#show ip bgp summary
BGP router identifier 85.0.0.1, local AS number 200
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor       V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.0.0.2        4   100       5       6        2    0    0 12:02:24 AM        2
4.0.0.2        4   100       6       5        2    0    0 12:02:24 AM        2
```

As you can see, Device1 establishes IBGP neighbors successfully with Device2 and Device3 respectively and Device4 establishes EBGP neighbors successfully with Device2 and Device3 respectively.

#Query the routing table of Device1.

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
         S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
[B]*> 55.0.0.0/24       0.0.0.0              0       32768 i
[B]*> 65.0.0.0/24       0.0.0.0              0       32768 i
[B]* i75.0.0.0/24       30.0.0.1             0    100      0 200 i
[B]*>i                  20.0.0.1             0    100      0 200 i
[B]* i85.0.0.0/24       30.0.0.1             0    100      0 200 i
[B]*>i                  20.0.0.1             0    100      0 200 i
```

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   75.0.0.0/24 [200/0] via 20.0.0.1, 1:13:17 AM, vlan2
B   85.0.0.0/24 [200/0] via 20.0.0.1, 1:13:17 AM, vlan2
```

As you can see, the routes 75.0.0.0/24 and 85.0.0.0/24 on Device1 select Device2 as the optimal next-hop device.

#Query the routing table of Device4.

```
Device4#show ip bgp
BGP table version is 2, local router ID is 85.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network           Next Hop          Metric LocPrf Weight Path
[B]*  55.0.0.0/24        3.0.0.2               0            0 100 i
[B]*>                  4.0.0.2               0            0 100 i
[B]*  65.0.0.0/24        3.0.0.2               0            0 100 i
[B]*>                  4.0.0.2               0            0 100 i
[B]*> 75.0.0.0/24        0.0.0.0               0        32768 i
[B]*> 85.0.0.0/24        0.0.0.0               0        32768 i

Device4#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   55.0.0.0/24 [20/0] via 4.0.0.2, 1:25:19 AM, vlan3
B   65.0.0.0/24 [20/0] via 4.0.0.2, 1:25:19 AM, vlan3
```

As you can see, the routes 55.0.0.0/24 and 65.0.0.0/24 on Device4 select Device3 as the optimal next-hop device.

Step 5:   Configure an ACL and route policy and set local-preference and metric.

#Configure Device2.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 75.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
```

```
Device2(config)#ip access-list standard 2
Device2(config-std-nacl)#permit 65.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map SetPriority1 10
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#set local-preference 110
Device2(config-route-map)#exi
Device2(config)#route-map SetPriority1 20
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 10
Device2(config-route-map)#match ip address 2
Device2(config-route-map)#set metric 100
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 20
Device2(config-route-map)#exit
```

Configure a route policy on Device2 to set the local-preference of the route 75.0.0.0/24 to 110 and the metric of the route 65.0.0.0/24 to 100.

#Configure Device3.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 85.0.0.0 0.0.0.255
Device3(config-std-nacl)#exit
Device3(config)#ip access-list standard 2
Device3(config-std-nacl)#permit 55.0.0.0 0.0.0.255
Device3(config-std-nacl)#exit
Device3(config)#route-map SetPriority1 10
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set local-preference 110
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority1 20
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 10
Device3(config-route-map)#match ip address 2
Device3(config-route-map)#set metric 100
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 20
Device3(config-route-map)#exit
```

Configure a route policy on Device3 to set the local-preference of the route 85.0.0.0/24 to 110 and the metric of the route 55.0.0.0/24 to 100.

NOTE

- In configuring a route policy, you can create a filtration rule based on a prefix list or ACL. The prefix list can precisely match routing masks while the ACL cannot match routing masks.

Step 6: Configure route policy for BGP.

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 route-map SetPriority1 out
Device2(config-bgp)#neighbor 3.0.0.1 route-map SetPriority2 out
Device2(config-bgp)#exit
```

Modify local-preference of 75.0.0.0/24 in the outgoing direction configured with the neighbor 10.0.0.1 on Device2, and modify metric of 65.0.0.0/24 in the outgoing direction configured with the neighbor 3.0.0.1.

#Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 route-map SetPriority1 out
Device3(config-bgp)#neighbor 4.0.0.1 route-map SetPriority2 out
Device3(config-bgp)#exit
```

Modify local-preference of 85.0.0.0/24 in the outgoing direction configured with the neighbor 10.0.0.1 on Device3, and modify metric of 55.0.0.0/24 in the outgoing direction configured with the neighbor 4.0.0.1.

The route policy configured on the peer may take effect only after BGP process is re-configured.

Step 7: Check the result.

#Query the routing table of Device1.

```
Device1#show ip bgp
BGP table version is 5, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network          Next Hop          Metric LocPrf Weight Path
[B]*> 55.0.0.0/24       0.0.0.0             0        32768 i
[B]*> 65.0.0.0/24       0.0.0.0             0        32768 i
[B]* i75.0.0.0/24       30.0.0.1            0    100      0 200 i
[B]*>i                20.0.0.1            0    110      0 200 i
[B]*>i85.0.0.0/24       30.0.0.1            0    110      0 200 i
[B]* i                20.0.0.1            0    100      0 200 i
```

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
     D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


B   75.0.0.0/24 [200/0] via 20.0.0.1, 12:01:34 AM, vlan2
B   85.0.0.0/24 [200/0] via 30.0.0.1, 12:00:51 AM, vlan3
```

As you can see, local-preference of the routes 75.0.0.0/24 and 85.0.0.0/24 is modified successfully. Device1 prefers the route 75.0.0.0/24 advertised by Device2 and the route 85.0.0.0/24 advertised by Device3.

#Query the routing table of Device4.

```
Device4#show ip bgp
BGP table version is 4, local router ID is 85.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network           Next Hop          Metric LocPrf Weight Path
[B]*  55.0.0.0/24        4.0.0.2              100           0 100 i
[B]*>                  3.0.0.2               0           0 100 i
[B]*> 65.0.0.0/24        4.0.0.2               0           0 100 i
[B]*                   3.0.0.2             100           0 100 i
[B]*> 75.0.0.0/24        0.0.0.0               0        32768 i
[B]*> 85.0.0.0/24        0.0.0.0               0        32768 i



Device4#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
     D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS


Gateway of last resort is not set


B   55.0.0.0/24 [20/0] via 3.0.0.2, 12:15:02 AM, vlan2
B   65.0.0.0/24 [20/0] via 4.0.0.2, 12:14:55 AM, vlan3
```

As you can see, metric of the routes 55.0.0.0/24 and 65.0.0.0/24 is modified successfully. Device4 prefers the route 55.0.0.0/24 advertised by Device2 and the route 65.0.0.0/24 advertised by Device3.

NOTE

- The route policy may be used in the outgoing direction of route advertisement or in the incoming direction of route receiving.

44.3.7 Configure BGP Confederation -E -A

Network Requirements

- Device2, Device3, Device4 and Device5 are in BGPAS200. To reduce IBGP full connections, they are distributed to two different AS in the same BGP confederation.
- Device1 establishes an EBGP neighbor with Device2 and advertises the route 100.0.0.0/24 to AS200.

Network Topology

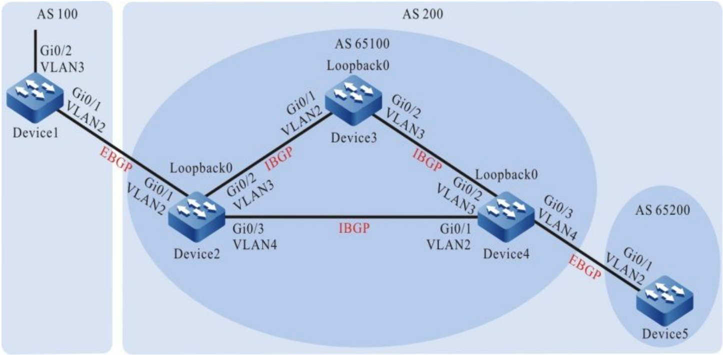


Figure 44-7 Networking for Configuring BGP Confederation

Equipment	Interface	VLAN	IP address
Device1	Gi0/1	2	1.0.0.1/24
	Gi0/2	3	100.0.0.1/24
Device2	Gi0/1	2	1.0.0.2/24
	Gi0/2	3	2.0.0.2/24
	Gi0/3	4	3.0.0.2/24
	Loopback0		20.0.0.1/32
Device3	Gi0/1	2	2.0.0.1/24
	Gi0/2	3	4.0.0.1/24
	Loopback0		30.0.0.1/32
Device4	Gi0/1	2	3.0.0.1/24

Equipment	Interface	VLAN	IP address
	Gi0/2	3	4.0.0.2/24
	Gi0/3	4	5.0.0.1/24
	Loopback0		40.0.0.1/32
Device5	Gi0/1	2	5.0.0.2/24

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF to make the Loopback routes between the devices are mutually reachable.

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 40.0.0.1 0.0.0.0 area 0
Device4(config-ospf)#exit
```

#Configure Device5.

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
Device5(config-ospf)#exit
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   4.0.0.0/24 [110/2] via 2.0.0.1, 12:02:42 AM, vlan3
              [110/2] via 3.0.0.1, 12:02:11 AM, vlan4
O   30.0.0.1/32 [110/2] via 2.0.0.1, 12:02:32 AM, vlan3
O   40.0.0.1/32 [110/2] via 3.0.0.1, 12:02:05 AM, vlan4
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   3.0.0.0/24 [110/2] via 2.0.0.2, 12:03:24 AM, vlan2
              [110/2] via 4.0.0.2, 12:02:38 AM, vlan3
O   20.0.0.1/32 [110/2] via 2.0.0.2, 12:03:24 AM, vlan2
O   40.0.0.1/32 [110/2] via 4.0.0.2, 12:02:38 AM, vlan3
```

#Query the routing table of Device4.

```
Device4#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   2.0.0.0/24 [110/2] via 3.0.0.2, 12:03:42 AM, vlan2
              [110/2] via 4.0.0.1, 12:03:42 AM, vlan3
O   20.0.0.1/32 [110/2] via 3.0.0.2, 12:03:42 AM, vlan2
O   30.0.0.1/32 [110/2] via 4.0.0.1, 12:03:42 AM, vlan3
```

#Query the routing table of Device5.

```
Device5#show ip route
```

```
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
   D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   2.0.0.0/24 [110/3] via 5.0.0.1, 12:00:03 AM, vlan2
O   3.0.0.0/24 [110/2] via 5.0.0.1, 12:00:03 AM, vlan2
O   4.0.0.0/24 [110/2] via 5.0.0.1, 12:00:03 AM, vlan2
O   20.0.0.1/32 [110/3] via 5.0.0.1, 12:00:03 AM, vlan2
O   30.0.0.1/32 [110/3] via 5.0.0.1, 12:00:03 AM, vlan2
O   40.0.0.1/32 [110/2] via 5.0.0.1, 12:00:03 AM, vlan2
```

As you can see, Device2, Device3 and Device4 learn each other's loopback routes.

Step 4: Configure the BGP connection in the confederation.

#Configure the IBGP connection in the confederation.

#Configure Device2.

```
Device2(config)#router bgp 65100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 65100
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 40.0.0.1 remote-as 65100
Device2(config-bgp)#neighbor 40.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 30.0.0.1 next-hop-self
Device2(config-bgp)#neighbor 40.0.0.1 next-hop-self
Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 65100
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 65100
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#neighbor 40.0.0.1 remote-as 65100
Device3(config-bgp)#neighbor 40.0.0.1 update-source loopback0
Device3(config-bgp)#exit
```

#Configure Device4.

```
Device4(config)#router bgp 65100
Device4(config-bgp)#neighbor 20.0.0.1 remote-as 65100
Device4(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device4(config-bgp)#neighbor 30.0.0.1 remote-as 65100
Device4(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device4(config-bgp)#exit
```

#Configure the EBGP connection in the confederation.

#Configure Device4.

```
Device4(config)#router bgp 65100
Device4(config-bgp)#neighbor 5.0.0.2 remote-as 65200
Device4(config-bgp)#exit
```

#Configure Device5.

```
Device5(config)#router bgp 65200
Device5(config-bgp)#neighbor 5.0.0.1 remote-as 65100
Device5(config-bgp)#exit
```

#Query the BGP neighbor state on Device4.

```
Device4#show ip bgp summary
BGP router identifier 40.0.0.1, local AS number 65100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
5.0.0.2         4   65200    15      15        2    0    0 00:09:40        0
20.0.0.1        4   65100     9       9        2    0    0 00:07:49        0
30.0.0.1        4   65100     7       7        2    0    0 12:05:39 AM        0
```

Device4 establishes IBGP neighbors with Device2 and Device3, and Device4 establishes an EBGP neighbor with Device5.

Step 5: Configure BGP connection.

#Configure Device1.

Configure an EBGP peer, with the AS number of confederation ID 200.

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#Configure Device2.

Configure the BGP confederation ID 200 and configure an EBGP peer, with the AS number of 100.

```
Device2(config)#router bgp 65100
Device2(config-bgp)#bgp confederation identifier 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#exit
```

#Configure Device3.

Configure BGP connection ID to 200.

```
Device3(config)#router bgp 65100
Device3(config-bgp)#bgp confederation identifier 200
Device3(config-bgp)#exit
```

#Configure Device4.

Configure the BGP confederation ID 200 and configure a confederation containing area 65100.

```
Device4#configure terminal
Device4(config)#router bgp 65100
Device4(config-bgp)#bgp confederation identifier 200
Device4(config-bgp)#bgp confederation peers 65200
Device4(config-bgp)#exit
```

#Configure Device5.

Configure the BGP confederation ID 200 and configure a confederation containing area 65200.

```
Device5(config)#router bgp 65200
Device5(config-bgp)#bgp confederation identifier 200
Device5(config-bgp)#bgp confederation peers 65100
Device5(config-bgp)#exit
```

Step 6: Check the result.

#Query the BGP neighbor state on Device1.

```
Device1#show ip bgp summary
BGP router identifier 100.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.0.0.2         4   200       6       6        2    0    0 00:02:20        0
```

As you can see, Device1 has successfully established EBGP neighborship with Device2.

#Query the route information on Device5.

```
Device5#show ip bgp
BGP table version is 49, local router ID is 5.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop            Metric LocPrf Weight Path
[B]*> 100.0.0.0/24       20.0.0.1                0    100      0 (65100) 100 i

Device5#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   100.0.0.0/24 [200/0] via 20.0.0.1, 12:00:38 AM, vlan2
```

Device5 successfully learns the route 100.0.0.0/24 and the next-hop attribute does not change when the route is transferred in the confederation. Device2, Device3, Device4 and Device5 belong to the same confederation, so the full connection relationship may not be established. Device5 obtains external route information through Device4.

44.3.8 Configure BGP to Link with BFD *-E -A*

Network Requirements

- Device1 establishes EBGP neighbors with Device2 and Device3 respectively, and Device2 establishes an IBGP neighbor with Device3.
- Device1 learns the EBGP route 3.0.0.0/24 from Device2 and Device3 simultaneously and Device1 prefers to forward data to the network segment 3.0.0.0/24 through Device2.
- Configure EBGP on Device1 and Device2 to link with BFD. After a fault occurs on the line between Device1 and Device2, BFD can quickly detect the fault and advertise to BGP. At this point. Device1 chooses to forward data to the network segment 3.0.0.0/24 through Device3.

Network Topology

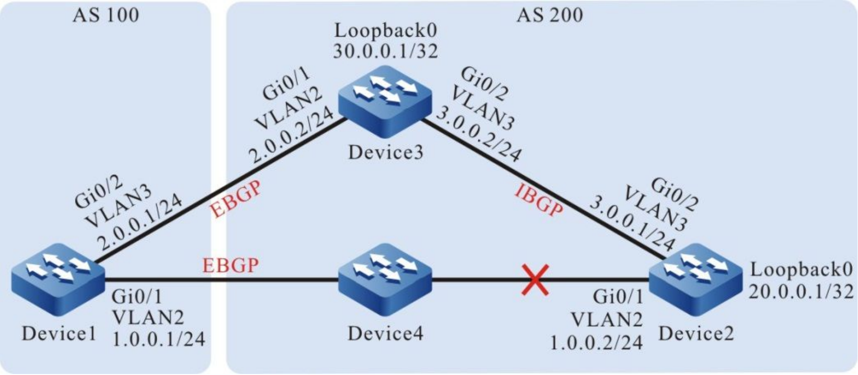


Figure 44-8 Networking for Configuring BGP to Link with BFD

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF to make the Loopback routes between the devices are mutually reachable.

#Configure Device2.

```
Device2#configure terminal
```

```
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   30.0.0.1/32 [110/2] via 3.0.0.2, 12:02:26 AM, vlan3
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   20.0.0.1/32 [110/2] via 3.0.0.1, 12:03:38 AM, vlan3
```

As you can see, Device2 and Device3 learn each other's loopback routes.

Step 4: Configure an ACL and route policy and set the route metric.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#route-map SetMetric
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set metric 50
Device1(config-route-map)#exit
```

Configure a route policy on Device1 to set the metric of the route 3.0.0.0/24 to 50.

Step 5: Configure BGP and associate a route policy on Device1.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#neighbor 2.0.0.2 remote-as 200
Device1(config-bgp)#neighbor 2.0.0.2 route-map SetMetric in
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 200
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#network 3.0.0.0 255.255.255.0
Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 200
Device3(config-bgp)#neighbor 2.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 200
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#network 3.0.0.0 255.255.255.0
Device3(config-bgp)#exit
```

The route policy configured on the peer may take effect only after BGP process is re-configured.

#Query the BGP neighbor state on Device1.

```
Device1#show ip bgp summary
BGP router identifier 2.0.0.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor       V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.0.0.2        4   200       2       2        2    0    0 12:01:32 AM        1
2.0.0.2        4   200       2       2        2    0    0 12:01:43 AM        1
```

#Query the BGP neighbor state on Device2.

```
Device2#show ip bgp summary
BGP router identifier 20.0.0.1, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.0.0.1         4   100       2       2        2    0    0 12:02:52 AM        0
30.0.0.1        4   200       3       3        2    0    0 12:02:45 AM        1
```

As you can see, BGP neighbors are established successfully among Device1, Device2 and Device3.

#Query the routing table of Device1.

```
Device1#show ip bgp
BGP table version is 3, local router ID is 1.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network          Next Hop            Metric LocPrf Weight Path
[B]*  3.0.0.0/24       2.0.0.2               50              0 200 i
[B]*>                  1.0.0.2               0               0 200 i

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   3.0.0.0/24 [20/0] via 1.0.0.2, 12:07:19 AM, vlan2
```

As you can see, the route 3.0.0.0/24 on Device1 selects Device2 as the optimal next-hop device.

Step 6: Configure BGP to link with BFD.

#Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 fall-over bfd
Device1(config-bgp)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#bfd min-receive-interval 500
Device1(config-if-vlan2)#bfd min-transmit-interval 500
Device1(config-if-vlan2)#bfd multiplier 4
Device1(config-if-vlan2)#exit
```

#Configure Device2.

```
Device2(config)#bfd fast-detect
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 fall-over bfd
```

```
Device2(config-bgp)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#bfd min-receive-interval 500
Device2(config-if-vlan20)#bfd min-transmit-interval 500
Device2(config-if-vlan2)#bfd multiplier 4
Device2(config-if-vlan2)#exit
```

Enable BFD between EBGP neighbors Device1 and Device2 and modify BFD to control the minimum send interval, minimum receive interval and detection timeout multiplier of the packets.

Step 7: Check the result.

#Query the BFD session state on Device1.

```
Device1#show bfd session
OurAddr          NeighAddr        LD/RD        State      Holddown     interface
1.0.0.1          1.0.0.2          2/2          UP         2000         vlan2
```

As you can see, BFD state on Device1 is correctly up and the holddown time is negotiated as 2000ms.

#When a fault occurs on the line between Device1 and Device2, the route can quickly switch to the backup line.

#Query the routing table of Device1.

```
Device1#show ip bgp
BGP table version is 6, local router ID is 1.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network         Next Hop         Metric LocPrf Weight Path
[B]*> 3.0.0.0/24       2.0.0.2            50          0 200 i

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set


B   3.0.0.0/24 [20/50] via 2.0.0.2, 12:00:05 AM, vlan3
```

As you can see, the next hop of the route 3.0.0.0/24 is switched to Device3.

45 IPv6 BGP

45.1 Overview

IPv6 BGP (BGP4+) is an extension of BGP-4, while BGP-4 can only manage the IPv4 route information. In order to support IPv6 protocol, IETF extends BGP-4 to form IPv6 BGP. The current IPv6 BGP standard is RFC 2858 (Multiprotocol Extensions for BGP-4).

IPv6 BGP needs to reflect the information about the IPv6 network layer protocol to NLRI (Network Layer Reachability Information) and NEXT_HOP attributes. Two NLRI attributes introduced to IPv6 BGP are:

- MP_REACH_NLRI: Multiprotocol Reachable NLRI, used to advertise the reachable routes and next hop.
- MP_UNREACH_NLRI: Multiprotocol Unreachable NLRI, used to revoke unreachable routes.

The NEXT_HOP attribute in IPv6 BGP is represented by an IPv6 address, which can be an IPv6 global unicast address or a link local address.

IPv6 BGP is applied in IPv6 network by means of the BGP attribute of multiprotocol extensions. The original message mechanism routing mechanism of BGP protocol have not changed.

45.2 IPv6 BGP Function Configuration

Table45-1 BGP Function List

Configuration task	
Configure an IPv6 BGP neighbor	Configure an IBGP neighbor
	Configure an EBGP neighbor
	Configure a passive BGP neighbor
	Configure an MP-BGP neighbor
	Configure BGP neighbor MD5 authentication
Configure BGP route generation	Configure BGP to advertise the local route
	Configure BGP route Re-distribution

Configuration task	
	Configure BGP to advertise the default route
Configure BGP route control	Configure BGP to advertise an aggregate route
	Configure the administrative distance of BGP route
	Configure route policy for the outgoing direction of BGP neighbor
	Configure route policy for the incoming direction of BGP neighbor
	Configure the maximum number of route entries received from BGP neighbor
	Configure the maximum number of BGP load balancing entries
Configure BGP route attributes	Configure BGP route weight
	Configure MED attribute of BGP route
	Configure Local-Preference attribute of BGP route
	Configure AS_PATH attribute of BGP route
	Configure NEXT-HOP attribute of BGP route
	Configure BGP route community attributes
Configure BGP network optimization	Configure BGP neighbor Keepalive time
	Configure BGP route scan time
	Configure EBGP neighbor fast failover
	Configure BGP route suppression
	Configure BGP neighbor refresh capability
	Configure BGP neighbor soft-reconfiguration capability

Configuration task	
	Configure BGP neighbor ORF capability
Configure BGP large network	Configure BGP peer group
	Configure BGP route reflector
	Configure BGP confederation
Configure BGP GR	Configure BGP GR Restarter
	Configure BGP GR Helper
Configure BGP to link with BFD	Configure EBGP to link with BFD
	Configure IBGP to link with BFD

45.2.1 Configure an IPv6 BGP Neighbor -E -A

Configuration Conditions

Before configuring a BGP neighbor, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- The network layer address of the interface is configured to make the adjacent node network layers accessible;

Configure an IBGP Neighbor

1. Basic configuration

Configuring the IBGP neighbor requires specifying the neighbor AS to be the same AS the device AS. The device can be configured with a Router ID that uniquely identifies a BGP device when establishing a BGP session. When Router ID is not configured, it will be selected by the device according to the interface address. The priority principle is as follows:

- Select the largest IP address of the Loopback interface as the Router ID;
- If the Loopback interface of IP address is not configured, select the largest IP address from other interfaces as the Router ID;
- Only when the interface is in the UP state can the interface address be selected as the Router ID.

Table 45-2 Configure an IBGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enable BGP and enter the BGP configuration mode	**router bgp** *autonomous-system*	Required By default, BGP is disabled
Configure BGP device ID	**bgp router-id** *router-id*	Optional By default, the device selects the ID according to the interface address in line with the principle of Loopback address priority and large IP address priority.
Configure an IBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no IBGP neighbor is created
Configure IBGP neighbor description	**neighbor** { *neighbor-address* | *peer-group-name* } **description** *description-string*	Optional By default, IBGP neighbor is not described
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Enable IBGP neighbor to send and receive IPv6 unicast route	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**	Optional By default, IBGP neighbor is disabled to send and receive IPv6 unicast route

2. Configure the Source Address of TCP Session

BGP uses TCP as its transport protocol. Characterized by reliable transport, TCP effectively ensures that BGP packets can be correctly transmitted to the neighbor.

Table 45-3 Configure the Source Address of TCP Session

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enable BGP and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure an IBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no IBGP neighbor is created
Configure the source address of IBGP neighbor TCP session	**neighbor** { *neighbor-address* | *peer-group-name* } **update-source** { *interface-name* | *ipv6-address* }	Required By default, the address of the route output interface is automatically selected as the source address of the TCP session.

NOTE

- The source address of TCP session needs to be explicitly configured between BGP neighbors in the presence of load balanced route. When the TCP source address is not configured, the BGP session may not be successfully established for a period of time due to the fact that the optimal route of the neighbors is different and different output interfaces are used as their respective source addresses.

Configure an EBGP Neighbor

1. Basic configuration

Configuring the EBGP neighbor requires specifying the neighbor AS that is different from the device AS.

Table45-4 Configure an EBGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable BGP and enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure an EBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no EBGP neighbor is created

2. Configure a non-direct EBGP neighbor

EBGP neighbors are in different operating networks and are usually connected by a direct physical link, so the default TTL value of IP packets for communication between EBGP neighbors is 1. The TTL value of the IP packets can be set by configuring a command between non-direct operating networks to connect BGP.

Table 45-5 Configure a Non-direct EBGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure an EBGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no EBGP neighbor is created
Configure the source address of EBGP neighbor TCP session	**neighbor** { *neighbor-address* | *peer-group-name* } **update-source** { *interface-name* | *ipv6-address* }	Optional By default, the address of the route output interface is automatically selected as the source address of the TCP session.
Configure to allow connection between EBGP neighbors	**neighbor** { *neighbor-address* | *peer-group-name* } **ebgp-multihop** [*ttl-value*]	Required By default, EBGP neighborship is not allowed between non-direct devices

Configure a Passive BGP Neighbor

The passive neighbor function of BGP is required for special applications. After applying the passive neighbor, the BGP does not initiate the TCP connection request to the neighbor to establish an BGP neighbor, and can only wait for the neighbor to initiate the connection request. By default, the neighbors will initiate connections with each other, and in the event of a conflict, a TCP connection will be preferred to form a BGP session. Before configuring a passive BGP neighbor, you need to configure a BGP neighbor.

Table 45-6 Configure a Passive BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a BGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no BGP neighbor is created.
Configure a passive BGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **passive**	Required By default, no passive neighbor is enabled

Configure an MP-BGP Neighbor

By default, a BGP neighbor needs to be activated to send and receive corresponding routes under the VRF address family and VPN address family. Before configuring an MP-BGP neighbor, you need to configure a BGP neighbor.

Table 45-7 Configure an MP-BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a BGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no BGP neighbor is created.
Enter the BGP IPv6 VRF configuration mode	**address-family ipv6 vrf** *vrf-name*	-
Configure a neighbor under the BGP IPv6 address family	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no BGP neighbor is created.
Activate the neighbor under the IPv6 VRF address family	**neighbor** { *neighbor-address* | *peer-group-name* } **activate**	Optional By default, the neighbor in the BGP IPv6 VRF configuration mode has been activated

Steps	Command	Description
Exit the BGP IPv6 VRF configuration mode	**exit-address-family**	-

NOTE

- A neighbor configured in BGP configuration mode and BGP IPv6 unicast configuration mode is a global neighbor, and a neighbor configured in BGP IPv6 VRF configuration mode belongs only to the VRF address family.

Configure BGP Neighbor MD5 authentication

BGP supports configuring MD5 authentication, which is done by TCP transport protocol, to protect information interactions between neighbors. Neighbors must have the same MD5 authentication key to establish a TCP connection, otherwise a TCP connection cannot be established after the MD5 authentication failure by the TCP transport protocol. Before configuring the BGP neighbor MD5 authentication, you need to configure a BGP neighbor.

Table 45-8 Configure BGP Neighbor MD5 Authentication

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a BGP neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **remote-as** *as-number*	Required By default, no BGP neighbor is created.
Configure BGP neighbor MD5 authentication	**neighbor** { *neighbor-address* | *peer-group-name* } **password** [0 | 7] *password-string*	Required By default, MD5 authentication is not made between BGP neighbors.

45.2.2 Configure IPv6 BGP Route Generation *-E -A*

Configuration Conditions

Before configuring the BGP route generation, ensure that:

- Enable BGP.

- Configure an IPv6 BGP neighbor and establish a session successfully.

Configure BGP to Advertise the Local Route

BGP can introduce a route from the IPv6 routing table to the BGP routing table through the network command. The route is introduced into the BGP routing table and published only if there are entries in the IPv6 routing table that match the network prefix and mask exactly.

When publishing a local route, you can either apply a route map to the route or specify the route as a backdoor route. The backdoor route treats an EBGP route as a local BGP route and uses the administrative distance of the local route to allow the IGP route to take precedence over the EBGP route, while the backdoor route is not advertised to the EBGP neighbor.

Table 45-9 Configure BGP to Advertise the Local Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure BGP to advertise the local route	**network** *ipv6-prefix* [**route-map** *rtmap-name* [**backdoor**] | **backdoor**]	Required By default, BGP does not advertise any local route

NOTE

- BGP advertises a local route with the route Origin attribute type of IGP.
- After applying the **network backdoor** command on the EBGP route, the administrative distance of the EBGP route will become that of the local route (by default, the administrative distance of EBGP route is 20 and of the local route is 200) and less than the default administrative distance of the IGP route, so that the IGP route is preferred and a backdoor link is formed between EBGP neighbors.
- The match options supported by the route map that is applied by BGP to advertise the local route include as-path, community, extcommunity, ipv6 address, ipv6 nexthop and metric, and the set options supported include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin and weight.

Configure BGP route Re-distribution

BGP is not primarily responsible for learning the route, but rather for controlling the route direction by managing the route attributes, so BGP generates a BGP route to advertise to the neighbor by redistributing the IGP. While redistributing the IGP route, BGP may apply the route map.

Table 45-10 Configure BGP Route Re-distribution

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure BGP to Re-distribute RIP routes	**redistribute** { **connected** | **isis** [*area-tag*] [**match** *isis-level*] | **ospf** *as-number* [**match** *route-sub-type*] | **rip** *process-id* | **static** } [**route-map** *map-name /* **metric** *value*]	Required By default, BGP does not Re-distribution any other IGP route

NOTE

- BGP advertises an IGP route with the route Origin attribute type of INCOMPLETE.
- The match options supported by the route map that is applied by BGP to Re-distribute other protocols include as-path, community, extcommunity, ipv6 address, ipv6 nexthop and metric, and the set options supported include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin and weight.

Configure BGP to Advertise the Default Route

BGP needs to introduce the default route before advertising it to a neighbor. There are two ways to introduce the default route: generate the default route through the **neighbor default-originate** command; Re-distribute the default route of other protocols through the **default-information originate** command.

The default route generated through the **neighbor default-originate** command is a route 0::/0 automatically generated through BGP and the default route Re-distributed through the **default-information originate** command is a route 0::/0 introduced by BGP to a Re-distributed protocol.

Table 45-11 Configure BGP to Advertise the Default Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure BGP to generate the default route	**neighbor** { *neighbor-address* | *peer-group-name* } **default-originate** [**route-map** *rtmap-name*]	Required By default, BGP does not generate the default route
Configure BGP to Re-distribute the default route of other protocols	**default-information originate**	Required By default, BGP does not Re-distribute the default route of other protocols

NOTE

- You also need to configure the route Re-distribution while configure BGP to Re-distribute the default route of other protocols.
- You may apply the route map to the default route when configuring BGP to generate the default route.
- The set options supported by the route map that is applied by BGP to generate the default route include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin and weight.

45.2.3 Configure IPv6 BGP Route Control *-E -A*

Configuration Conditions

Before configuring the BGP route control, ensure that:

- Enable BGP.
- Configure an IPv6 BGP neighbor and establish a session successfully.

Configure BGP to Advertise an Aggregate Route

In a large BGP network, you need to configure a BGP aggregate route to reduce the number of routes advertised to the neighbor or to effectively control the BGP routing process.

Table 45-12 Configure BGP to Advertise an Aggregate Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure BGP to advertise an aggregate route	**aggregate-address** *ipv6-prefix* [**as-set** / **summary-only** / **route-map** *rtmap-name*]	Required By default, BGP will not perform route aggregation.

NOTE

- When BGP advertises an aggregate route, you can reduce the size of the route advertisements by specifying the **summary-only** command option to advertise only the aggregate route.
- An aggregate route with the AS_PATH attribute can be generated by specifying the **as-set** command option.
- You may set richer attributes of the aggregate route by applying the route map to the aggregate route.

Configure the Administrative Distance of BGP Route

In the IP routing table, each protocol has an administrative distance to control routing, the smaller the value, the higher the priority. BGP influences the routing by configuring the administrative distance to the specified network segment. The administrative distance covering the route to the specified network segment will be modified. Meanwhile, ACL can be applied to effectively filter the covered network segment. Only the administrative distance that the ACL allows for network segments is modified.

The **distance bgp** command is used to modify the administrative distance of the external and internal routes of BGP and the local routes, while the **distance** command is only used to modify the administrative distance of the routes in the specified network segments. The **distance** command takes precedence over the **distance bgp** command. A network segment covered by the **distance** will use the administrative distance specified by the command, while an uncovered network segment will use the administrative distance set by **distance bgp**.

Table 45-13 Configure the Administrative Distance of BGP Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure BGP to modify the default administrative distance	**distance bgp** *external-distance internal-distance local-distance*	Optional By default, the administrative distance of EBGP route is 20, of IBGP route is 200 and of local route is 200.
Configure the administrative distance for a specified network segment	**distance** *administrative-distance ipv6-prefix* [*acl-num* | *acl-name*]	

Configure Route Policy for the Outgoing Direction of BGP Neighbor

The BGP route advertisement or routing is accomplished by its powerful route attributes. When advertising routes to a neighbor, you may modify the route attributes by corresponding policies or filter some routes. The policies currently supported for application in the outgoing direction are:

- distribute-list;
- filter-list: filter-list of AS_PATH properties;
- prefix-list: IP prefix-list;
- Route-map: Route Map.

Table 45-14 Configure Route Policy for the Outgoing Direction of BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-

Steps	Command	Description
Specify the distribute-list to be applied in the outgoing direction	**neighbor** { *neighbor-address* | *peer-group-name* } **distribute-list** {*access-list-num* | *access-list-name* } **out**	Multiple choice (the distribute-list and IP prefix-list cannot be configured simultaneously) By default, the route policy for the outgoing direction of BGP neighbor is not configured.
Specify the AS_PATH attribute filter-list to be applied in the outgoing direction	**neighbor** { *neighbor-address* | *peer-group-name* } **filter-list** *aspath-list-name* **out**	
Specify the IP prefix-list to be applied in the outgoing direction	**neighbor** { *neighbor-address* | *peer-group-name* } **prefix-list** *prefix-list-name* **out**	
Specify the route map to be applied in the outgoing direction	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **out**	

NOTE

- The route policy configured for the outgoing direction of BGP neighbor can take effect only after the neighbor is set.
- When configuring the route map applied in the outgoing direction of the route reflector, you can only change the NEXT-HOP attributes.
- Refer to the PBR Tools -Configure AS-PATH list to configure the filter-list.
- Multiple policies can be configured in the outgoing direction of the neighbor simultaneously and applied by BGP in the sequential order of **distribute-list**, **filter-list**, **prefix-list** and **route-map**. After the first policy is rejected, the next policy is not applied, and the route information is not advertised until all the configured policies have passed.
- The match options supported by the route map that is applied in the outgoing direction of BGP include as-path, community, extcommunity, ipv6 address, ipv6 nexthop and metric, and the set options supported include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin and weight.

Configure Route Policy for the Incoming Direction of BGP Neighbor

BGP can apply policies to filter or modify the attributes of received route information. Like the outgoing direction, the incoming direction also supports four policies:

- distribute-list;
- filter-list: filter-list of AS_PATH properties;
- prefix-list: IPv6 prefix-list;
- Route-map: Route Map.

Table 45-15 Configure Policy for the Incoming Direction of BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Specify the distribute-list to be applied in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **distribute-list** { *access-list-num* | *access-list-name* } **in**	Multiple choice (the distribute-list and IP prefix-list cannot be configured simultaneously) By default, no policy is specified in the incoming direction
Specify the AS_PATH attribute filter-list to be applied in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **filter-list** *aspath-list-name* **in**	
Specify the IP prefix-list to be applied in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **prefix-list** *prefix-list-name* **in**	
Specify the route map to be applied in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in**	

NOTE

- The route policy configured for the incoming direction of BGP neighbor can take effect only after the neighbor is set.
- Multiple policies can be configured in the incoming direction of the neighbor simultaneously and applied by BGP in the sequential order of **distribute-list**, **filter-list**, **prefix-list** and **route-map**. After the first policy is rejected, the next policy is not applied, and the route is added to the database only all configured policies have passed.
- The match options supported by the route policy that is applied in the incoming direction of BGP include as-path, community, extcommunity, ipv6 address, ipv6 nexthop and metric, and the set options supported include as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin and weight.

Configure the Maximum Number of Route Entries Received from BGP Neighbor

The BGP device supports limiting the number of route entries received from a specified neighbor and gives an alarm or is disconnected when the number of routes received from the specified neighbor reaches a certain threshold.

Table 45-16 Configure the Maximum Number of Route Entries Received from BGP Neighbor

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure the maximum number of route entries received from a neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **maximum-prefix** *prefix-num* [*threshold-value*] [**warning-only**]	Required By default, the number of prefix entries received from a neighbor is not limited.

NOTE

- If the **warning-only** command option is not specified, when the number of routes received by a neighbor by BGP reaches the maximum number of entries, the BGP session will be disconnected automatically.
- If the **warning-only** command option is specified, when the number of routes received by a neighbor by BGP reaches the maximum number of entries, BGP gives a warning message only and does not prevent the routes from continuing to learn.

Configure the Maximum Number of BGP Load Balancing Entries

In a BGP networking environment, if there are several paths with the same overhead to the same destination, a load balanced route can be formed by configuring the number of BGP load entries.

Table 45-17 Configure the Maximum Number of BGP Load Balancing Entries

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-

Steps	Command	Description
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure the maximum number of IBGP load balancing entries	**maximum-paths ibgp** *number*	Required By default, IBGP does not perform the load balanced routing
Configure the maximum number of EBGP load balancing entries	**maximum-paths** *number*	Required By default, EBGP does not perform the load balanced routing

NOTE

- After the maximum number of BGP load balancing entries is configured, the load can be formed only when the EBGP route is preferred.
- The command for the configuration of the maximum number of load balancing entries is different in different BGP configuration modes, as shown in the description of the **maximum-paths** in BGP technical command.

45.2.4 Configure IPv6 BGP Route Attributes *-E -A*

Configuration Conditions

Before configuring the BGP route attributes, ensure that:

- Enable BGP.
- Configure an IPv6 BGP neighbor and establish a session successfully.

Configure BGP Route Weight

The first rule for BGP routing is to compare the weight value of the routes. The greater the weight value of the route, the higher the priority. The route weight value is a local attribute of the device and is not passed to other BGP neighbors. The route weight values range from 0 to 65535. By default, the weight value of the routes learnt from a neighbor is 0 and of all routes generated by the local device is 32768.

Table 45-18 Configure BGP Route Weight

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the route weight of a neighbor or peer group	**neighbor** { *neighbor-address* | *peer-group-name* } **weight** *weight-num*	Required By default, the route weight of a neighbor is 0

Configure MED Attribute of BGP Route

The MED attribute is used to select the best route for traffic entering AS. Under the same routing conditions, when BGP learns the routes with the same destination but different next hop from different EBGP neighbors, it will prefer the route with the minimum MED as the best entry.

MED is sometimes referred to as an "external metric" and is marked as "Metric" in the BGP routing table. BGP will advertise the MED attributes of the route learnt from the neighbor to the IBGP neighbors, but not to the EBGP neighbors, so MED is only applicable between the neighbor AS.

1. Configure BGP to compare MED of the routes from different AS neighbors

By default, BGP will only perform MED routing for routes learnt from the same AS, but can ignore the restrictions on the same AS requirements in MED routing through the command **bgp always-compare-med**.

Table 45-19 Configure BGP to Compare MED of the Routes from Different AS Neighbors

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to compare MED of the routes from different AS neighbors	**bgp always-compare-med**	Required By default, BGP is only allowed to compare the MED of routes from the same AS.

2. Configure BGP to sort MED according to the route grouping by AS_PATH

By default, MED sorting by BGP according to the route grouping by AS_PATH is disabled. This function can be enabled through the command **bgp deterministic-med**. In route selection, all routes are arranged based on AS_PATH. In each AS_PATH group, the routes are sorted according to the size of MED. The route with the smallest MED value is selected as the best route of this group.

Table 45-20 Configure BGP to Sort MED according to the Route Grouping by AS_PATH

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
BGP sorts MED according to the route grouping by AS_PATH	**bgp deterministic-med**	Required By default, MED sorting by BGP according to the route grouping by AS_PATH is disabled.

3. Configure to compare MED of routes in the local confederation

EBGP routes from different AS do not compare MED attributes by default. This principle is also valid for the EBGP in the confederation. The command **bgp bestpath med confed** is used to compare the MED attribute value of the routes in the local confederation.

Table 45-21 Configure BGP to Compare MED of Routes in the Local Confederation

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure BGP to compare MED attribute value of routes in the local confederation	**bgp bestpath med confed**	Required By default, the MED attribute value of routes in the local confederation will not be compared.

4. Configure a Route Map to Modify MED Attribute

When receiving and sending routes, you can use the route map to modify the MED attribute value.

Table 45-22 Configure a Route Map to Modify MED Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure a route map to modify MED attribute	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in | out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the MED attribute, you need to modify MED through the **set metric** command. See PBR Tools - Technical manual -**set metric**.
- After configuring the command **neighbor attribute-unchanged**, you cannot change the neighbor MED attribute through the route map.

Configure Local-Preference Attribute of BGP Route

The Local-Preference attribute is passed only between IBGP neighbors. Local-Preference is used to select the best exit from AS, and the route with the largest Local-Preference will be preferred.

The Local-Preference value ranges from 0 to 4294967295, the higher the value, the higher the priority of the route. By default, the Local-Preference attribute of all routes advertised to the IBGP neighbors is 100 and the Local-Preference attribute can be modified through **bgp default local-preference** or road map.

1. Configure BGP to modify the default Local-Preference attribute

Table 45-23 Configure BGP to Modify the Default Local-Preference Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-

Steps	Command	Description
Configure the default Local-Preference attribute of BGP	**bgp default local-preference** *local-value*	Optional By default, the default local priority is 100.

2. Configure a route map to modify the Local-Preference attribute

Table 45-24 Configure a Route Map to Modify the Local-Preference Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure a route map to modify the Local-Preference attribute	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in | out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the Local-Preference attribute, you need to modify Local-Preference attribute through the command **set local-preference**. See PBR Tools - Technical manual -**set local-preference**.

Configure AS_PATH Attribute of BGP Route

1. Configure to ignore AS_PATH comparison in BGP routing

Under other same conditions, the route with the shortest AS_PATH will be preferred in the BGP routing, but the routing through AS_PATH can be canceled through the command **bgp bestpath as-path ignore**.

Table 45-25 Configure to Ignore AS_PATH Comparison in BGP Routing

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to ignore AS_PATH comparison in BGP routing	**bgp bestpath as-path ignore**	Required By default, AS_PATH attribute value is compared in routing.

2. Configure the number of repeats of local AS number allowed by BGP

To avoid routing loops, BGP will check the AS_PATH attribute of the routes received from the neighbors and discard the routes containing local AS number. Through the command **neighbor allowas-in**, the routes received by BGP are allowed to contain the local AS number in the AS_PATH attribute and the number of routes containing the local AS number may be configured.

Table 45-26 Configure the Number of Repeats of Local AS Number Allowed by BGP

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure the number of repeats of local AS number	**neighbor** { *neighbor-address* | *peer-group-name* } **allowas-in** [*as-num*]	Required By default, a route received from a neighbor is not allowed to have a local AS number in the AS_PATH attribute

3. Configure to remove private AN number when BGP advertises routes to neighbors

In a large BGP network, the route AS_PATH attribute has a confederation or community attribute. By default, BGP will carry this private AS attribute information when it advertises to its neighbors. To block the private network information, you may remove the private AS number through **neighbor remove-private-AS**.

Table 45-27 Configure to Remove Private AN Number when BGP advertises Routes to Neighbors

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure to remove private AN number when BGP advertises routes to neighbors	**neighbor** { *neighbor-address* | *peer-group-name* } **remove-private-AS**	Required By default, BGP will carry a private AS number when it advertises to its neighbors.

4. Configure to Detect the Validity of the First AS Number of EBGP Route

When BGP advertises a route to an EBGP neighbor, the local AS number is pressed into the start position of AS_PATH. The first AS that advertises the route will be at the last position. Normally, the first AS number of the route received from EBGP should be the same as the neighbor's AS number, or the route will be discarded.

Table 45-28 Configure to Detect the Validity of the First AS Number of EBGP Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to detect the validity of the first AS number of EBGP route	**bgp enforce-first-as**	Required By default, this first AS number check mechanism is disabled for BGP.

5. Configure a Route Map to Modify the AS_PATH Attribute

BGP supports to configure a route map to modify the AS_PATH attribute. The route attributes may be prepended through **set as-path prepend**, so as to affect the neighbor routing. In using **set as-path prepend**, the local AS is preferred to prepend AS_PATH. If another AS is used, enough attention must be paid to avoid the route advertisements to that AS being rejected.

Table 45-29 Configure a Route Map to Modify the AS_PATH Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure a route map to modify the AS_PATH attribute	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in | out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the AS_PATH attribute, you need to modify the AS_PATH attribute through the command **set as-path prepend**. See PBR Tools - Technical manual - **set as-path**.

Configure NEXT-HOP Attribute of BGP Route

When BGP advertises a route to an IBGP neighbor, the route attributes will not be changed (including next-hop attribute). When BGP advertises the route learnt from an EBGP neighbor to an IBGP neighbor, the next-hop attribute of the route advertised to the BGP neighbor is the local IPv6 address through the command **neighbor next-hop-self**. BGP also supports the use of a road map to modify the next-hop attribute.

1. Configure BGP to Use the Local IP Address as the Next Hop of the Route

Table 45-30 Configure BGP to Use the Local IP Address as the Next Hop of the Route

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-

Steps	Command	Description
Configure BGP to use the local IP address as the next hop when advertising a route to the neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **next-hop-self**	Required By default, the next-hop attribute advertised to the EBGP neighbor is the local IPv6 address and advertised to the IBGP will be maintained and not be changed.

NOTE

- When BGP is configured to use the local IPv6 address as the next hop of the route, if the source address of the TCP session is configured using **neighbor update-source**, the source address will be used as the next-hop address; otherwise, the output interface IP of the advertising device will be selected as the local IPv6 address.

2. Configure a Route Map to Modify the NEXT-HOP Attribute

BGP supports the configuration of a route map to modify the NEXT-HOP attribute and the next-hop attribute can be modified through **set ipv6 next-hop**.

Table 45-31 Configure a Route Map to Modify the NEXT-HOP Attribute

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure a route map to modify the NEXT-HOP attribute	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in | out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the NEXT-HOP attribute, you need to modify the NEXT-HOP attribute through the command **set ipv6 next-hop**. See PBR Tools - Technical manual - **set ipv6 next-hop**.

Configure BGP route Community Attributes

BGP supports configuration to send the community attributes when advertising the routes to a neighbor. The route map can be applied on the specified neighbor to match the community attributes in both incoming and outgoing directions.

The community attributes are used to identify a set of routes to apply the route policy on the routes. The community attributes are in two forms, standard and extended. The standard community attribute is 4 bytes long, including NO_EXPORT, LOCAL_AS, NO_ADVERTISE and INTERNET; the extended community attribute is 8 bytes long, including Route Target (RT) and Route Origin.

1. Configure BGP to advertise the route community attributes to neighbors

The **neighbor send-community** supports advertisements of the standard or extended community attributes, or both, to the neighbors.

Table 45-32 Configure BGP to Advertise the Route Community Attributes to Neighbors

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure to advertise the route community attributes to neighbors	**neighbor** { *neighbor-address* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]	Required By default, no community attribute is advertised to any neighbor.

NOTE

- After activating a neighbor under VPNv6 address family, BGP will automatically advertise the standard and extended community attributes to the neighbor.

2. Configure a Route Map to Modify the Community Attributes

BGP supports the configuration of a route map to modify the community attributes, and the community attributes may be modified through **set communtiy**.

Table 45-33 Configure a Route Map to Modify the Community Attributes

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure a route map to modify the community attributes	**neighbor** { *neighbor-address* | *peer-group-name* } **route-map** *rtmap-name* **in | out**	Required By default, no route map is applied to any neighbor

NOTE

- When configuring a road map to modify the community attributes, you need to modify the community attributes through the command **set communtiy**. See PBR Tools - Technical manual -**set communtiy**.

45.2.5 Configure IPv6 BGP Network Optimization *-E -A*

Configuration Conditions

Before configuring the BGP network optimization, ensure that:

- Enable BGP.
- Configure an IPv6 BGP neighbor and establish a session successfully.

Configure BGP Neighbor Keepalive time

After successful establishment of a BGP session, neighbors will periodically send Keepalive messages to maintain the BGP session relationship. BGP session will be disconnected over time if no Keepalive message or route update is received from the neighbor within the session Holdtime. The session Keepalive time will not exceed one third of the Holdtime.

Table 45-34 Configure Keepalive Time of a BGP Neighbor

Steps	Command	Description

Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure the global BGP Keepalive time and Holdtime	**timers bgp** *keepalive-interval holdtime-interval*	Optional By default, the Keepalive timer interval is 60s, the hold-down timer interval is 180s and the session reconnection timer interval is 120s.
Configure the Keepalive time and Holdtime of a BGP neighbor or peer group	**neighbor** { *neighbor-address* | *peer-group-name* } **timers** { *keepalive-interval holdtime-interval* | **connect** *connect-interval* }	

NOTE

- The Keepalive time and Holdtime configured for the specified neighbor take precedence over the global BGP Keepalive time and Holdtime.
- After neighbor negotiation, the minimum Holdtime will be used as the Holdtime of the BGP session.
- When both the Keepalive time and Holdtime are configured to zero, the neighbor Keepalive/hold function will be disabled.
- When the Keepalive interval exceeds one third of the Holdtime, BGP will send a Keepalive packet using one third of the Holdtime.

Configure BGP Route Scan Time

BGP mainly completes the pathfinding process with AS the unit, and IGP completes the internal pathfinding of AS, so BGP route usually relies on IGP route. After the next hop or output interface of the IGP route on which GGP relies changes, BGP updates the BGP route by regularly scanning the IGP route and completes the local BGP route update in the scan cycle.

Table 45-35 Configure BGP Route Scan Time

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-

Configure BGP route scan time	**bgp scan-time** *time*	Optional By default, the BGP route scan time is 60s.

NOTE

- Too short BGP route scan time will make BGP frequently scan the route, affecting the device performance.

Configure EBGP Neighbor Fast Failover

After successful establishment of a BGP session, neighbors will periodically send Keepalive messages to each other to maintain the BGP session relationship. BGP session will be disconnected over time if no Keepalive message or route update is received from the neighbor within the session Holdtime. You can configure a direct EBGP neighbor to immediately disconnect the BGP when the connection interface is down without waiting for the BGP Keepalive timeout. When the EBGP neighbor fast failover is canceled, the EBGP session will not respond to the interface down and the BGP session connection will be disconnected through a timeout.

Table 45-36 Configure EBGP neighbor fast failover

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure EBGP neighbor fast failover	**bgp fast-external-failover**	Optional By default, the rapid processing of EBGP in response to direct interface down has been enabled.

Configure BGP Route Suppression

Frequent oscillating routes in the network will cause network instability. BGP can suppress such routes by configuring route dampening to reduce the impact of oscillating routes on the network.

Frequent oscillating routes will be allocated with an increased penalty value. When the penalty value exceeds the suppress limit, the route will not be advertised to the neighbor, and the penalty value cannot exceed the maximum suppression time. When a route does not oscillate during the half-life, the penalty value is halved, and the route is not re-advertised to the neighbor until the value is below the reuse limit.

- Half-life: the time it takes for the route penalty value to be halved.
- Reuse limit: the threshold value used for route recovery.
- Suppress limit: the threshold at which a route is suppressed.
- Maximum suppression time: the maximum time for a route to be suppressed.

Table 45-37 Configure BGP Route Suppression

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure the BGP route dampening cycle	**bgp dampening** [*reach-half-life* [*reuse-value suppress-value max-suppress-time* [*unreach-half-life*]] | **route-map** *rtmap-name*]	Required By default, the route suppression is disabled. For the enabled default route, the suppression half-life is 15min, the reuse limit is 750, the suppress limit is 2000, the maximum suppression time is 60min and the unreachable half-life of the route penalty is 15min.

NOTE

- The route oscillations include route additions/deletions and route attribute changes, such as next hop and MED attributes.

Configure BGP Neighbor Refresh Capability

When the route policy applied on a BGP neighbor changes, the routing table shall be refreshed again. One method is to restart the session by resetting the BGP connection to reset, which will result in the BGP route oscillation and affect the service operation. The other more graceful method is to configure the local BGP device to support the route refresh capability. When its neighbor needs to reset the route, a Route-Refresh message is advertised to the local device. After receiving the Route-Refresh message, the local device resends the route to the neighbor to achieve dynamic refresh of the routing table without disconnecting the BGP session.

Table 45-38 Configure BGP Neighbor Refresh Capability

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure to enable the neighbor refresh capability	**neighbor** { *neighbor-address* | *peer-group-name* } **capability route-refresh**	Optional By default, advertisement to the neighbor to support the route refresh capability has been enabled.

Configure BGP Neighbor Soft-Reconfiguration Capability

When the route policy applied on a BGP neighbor changes, the routing table shall be refreshed again. One method is to restart the session by resetting the BGP connection to reset, which will result in the BGP route oscillation and affect the service operation. Another more graceful method is to configure the local BGP device to support the route refresh capability. Another method is to enable the soft-reconfiguration capability of the local BGP device. By default, the BGP device keeps the route information of all neighbors. After enabling the soft-reconfiguration capability of the neighbors, it will refresh the routes of the neighbors kept locally without disconnecting BGP session.

Table 45-39 Configure BGP Neighbor Soft-Reconfiguration Capability

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure to enable the neighbor soft-reconfiguration capability	**neighbor** { *neighbor-address* | *peer-group-name* } **soft-reconfiguration inbound**	Required By default, the neighbor soft-reconfiguration is disabled.

Configure BGP Neighbor ORF Capability

BGP implements precise route control through rich route attributes, which is usually achieved by applying routing policies in both incoming and outgoing directions and is the behavior of the BGP locally. BGP also supports ORF (Outbound Route Filtering) capability. Through the Route-refresh packet, it advertises the local entry policy to the neighbors and the neighbors advertise the application of the policy to BGP, so as to greatly reduce the interaction of the route update packets between the BGP neighbors.

Successful ORF capability negotiation requires the following:

- Both neighbors need to enable the ORF capability;
- ORF send and ORF receive must be paired. That, if one neighbor is ORF send, the other must be ORF both or ORF receive; if one is ORF receive, the other must be ORF send or ORF both;
- The neighbor using ORF send needs to apply the prefix-list in the incoming direction.

Table 45-40 Configure BGP Neighbor ORF Capability

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure a neighbor to apply prefix-list in the incoming direction	**neighbor** { *neighbor-address* | *peer-group-name* } **prefix-list** *prefix-list-name* **in**	Required By default, no prefix-list is applied on any BGP neighbor.
Configure a neighbor to support ORF	**neighbor** { *neighbor-address* | *peer-group-name* } **capability orf prefix-list** { **both** | **receive** | **send** }	Required By default, no neighbor advertisement to support ORF is enabled.

45.2.6 Configure IPv6 BGP Large Network *-E -A*

Configuration Conditions

Before configuring BGP large network, ensure that:

- Enable BGP;
- Configure an IPv6 BGP neighbor and establish a session successfully.

Configure BGP Peer Group

A BGP peer group is a collection of BGP neighbors with the same configuration policy, and any configuration for a peer group will affect all peer members at the same time. Configuring the BGP peer group facilitates centralized management and maintenance of neighbors.

Table 45-41 Configure a BGP Peer Group

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Create a BGP peer group	**neighbor** *peer-group-name* **peer-group**	Required By default, no peer group is configured and the neighbors do not join any peer group.
Configure a neighbor to join a peer group	**neighbor** *neighbor-address* **peer-group** *peer-group-name*	

NOTE

- The configuration of a peer group affects all peer group members simultaneously.
- The same configuration as the peer group will be deleted when a neighbor joins the peer group.
- When a route policy is configured for the outgoing or incoming direction of a peer group, after the route policy changes, it will not be effective for the neighbors that have joined the peer group. The changed route policy can be effective for the peer group members only after the peer group is re-configured.

Configure BGP Route Reflector

In a large BGP networking environment, the whole network connection of IBGP neighbors is required, that is, each BGP establishes connection with all other IBGP neighbors, so the number of BGP connections in the networking environment of N BGP neighbors is N*(n-1)/2. The greater the number of connections, the greater the number of route advertisements. The BGP route reflector is a way to reduce the number of network connections. It divides several IBGPs into a group and specifies a BGP as the reflector (RR), the other BGPs as the clients, and the BGP in the non-group as the non-client.

The client only peers with RR and not with other BGPs, thereby reducing the number of necessary IBGP connections to N-1.

Route reflection principle of BGP route reflector:

- Routes learnt from non-client IBGP neighbors are reflected to clients only;
- Routes learnt from clients are reflected to all clients and non-clients except the client that initiates the route;
- Routes learnt from the neighbors are reflected to all clients and non-clients.

Table 45-42 Configure BGP Route Reflector

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Configure a reflector cluster ID	**bgp cluster-id** { *cluster-id-in-ip* | *cluster-id-in-num* }	Required By default, the device Router ID is used as the reflector cluster ID.
Configure a neighbor as the reflector client	**neighbor** { *neighbor-address* | *peer-group-name* } **route-reflector-client**	Required By default, no neighbor is specified as the reflector client.
Configure the BGP client-to-client reflection	**bgp client-to-client reflection**	Optional By default, the BGP route client-to-client reflection has been enabled.

NOTE

- The reflector cluster ID is used to identify the same reflector area in which multiple reflectors may exist and have the same reflector cluster ID.

Configure BGP Confederation

In a large BGP networking environment, the whole network connection of IBGP neighbors is required, that is, each BGP establishes connection with all other IBGP neighbors, so the number of BGP connections in the networking environment of N BGP neighbors is N*(n-1)/2. The greater the number of connections, the greater the number of route advertisements. BGP confederation is another method to reduce the number of network connections. With the divide-and-rule policy, it divides an AS into several sub-AS areas. Each AS area form a confederation. The confederations are fully connected through IBGP. The sub-AS areas in a confederation are connected by EBGP, effectively reducing the number of BGP connections.

When configuring a BGP confederation, you need to assign a confederation ID to each confederation and specify its members. The confederation is different from the route reflector. Under the route reflector conditions, only the route reflector is required to support the route reflection, while the confederation requires all members to support the confederation function.

Table 45-43 Configure BGP Confederation

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Create the BGP confederation ID	**bgp confederation identifier** *as-number*	Required By default, no confederation AS number is configured.
Configure a confederation member	**bgp confederation peers** *as-number-list*	Required By default, no confederation sub-AS number is configured.

NOTE

- The confederation ID is used to identify the confederation sub-AS and the confederation members are distributed to the sub-AS.

45.2.7 Configure IPv6 BGP GR *-E -A*

GR (Graceful Restart) is used to keep the route information at the forwarding level of the local device and neighbor device unchanged and the forwarding not affected during the master-backup switching; after the device switching and re-running, the two devices synchronize the route information at the protocol level and update the forward layer, so as to achieve the purpose of uninterrupted data forwarding during the switching process.

Roles in GR process:

- GR Restarter: a device that performs protocol GR.
- GR Helper: a device that helps the protocol GR.
- GR Time: maximum restart time of GR-Restarter. The GR Helper only keeps the route

stable for that time.

Dual-master control devices can serve as GR Restarter and GR Helper, while centralized devices can only serve as GR Helper to assist the Restarter end to complete GR. When GR Restarter performs GR, the GR Helper maintains its route until the GR Time expires. After assisting the GR Restarter in completing GR, the GR Helper synchronizes the route message. In this period, the network route and packet forwarding remain in the state before GR, effectively guaranteeing the network stability.

The BGP GR relationship is established by OPEN packet negotiation when neighbors are connected. When the GR Restarter neighbor restarts, the BGP session is disconnected, but the routes learnt from that neighbor are not deleted and are still forwarded normally in the IP routing table. These routes are only marked Stale in the BGP routing table and will be updated after GR completion or timeout.

GR Restarter needs to complete the connection with the GR Helper within the maximum allowed time (**restart-time**), otherwise, the GR Helper will remove the remaining GR routes and remove the GR process. After the neighbor reconnection, the GR Helper needs to receive the update packet with End-Of-RIB tag from the GR Restarter to complete the GR process successfully; otherwise, the GR routes not updated will be deleted after the maximum Holdtime (stalepath-time) and the GR relationship will be canceled.

Configuration Conditions

Before configuring the BGP GR, ensure that:

- Enable BGP.
- Configure an IPv6 BGP neighbor and establish a session successfully.

Configure BGP GR Restarter

Table 45-44 Configure BGP GR Restarter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enable the BGP GR capability	**bgp graceful-restart** [**restart-time** *time* | **stalepath-time** *time*]	Required By default, the GR capability of the BGP device is disabled. The maximum allowed time for the session re-establishment of the default neighbors with enabled GR is 120s and the maximum Holdtime of the GR route is 360s.

Steps	Command	Description
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure advertisement of the GR-Restarter capability to the neighbor	**neighbor** { *neighbor-address* | *peer-group-name* } **capability graceful-restart**	Required By default, the GR Restarter capability is not advertised to the neighbor.

Configure BGP GR Helper

Table 45-45 Configure BGP GR Helper

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enable the BGP GR capability	**bgp graceful-restart** [**restart-time** *time* | **stalepath-time** *time*]	Required By default, the GR capability of the BGP device is disabled. The maximum allowed time for the session re-establishment of the default neighbors with enabled GR is 120s and the maximum Holdtime of the GR route is 360s.

45.2.8 Configure IPv6 BGP to Link with BFD *-E -A*

In general, there are other intermediate devices running between BGP neighbors. When these intermediate devices fail, the BGP session is still normal in Holdtime and cannot respond to the link failure of intermediate devices in a timely manner. BFD provides a method for quickly detecting the state of the line between two devices. When BFD detection is enabled between the BGP devices, if there is a line fault between the devices, BFD will quickly detect the line fault, notify BGP, trigger BGP to quickly disconnect the session and switch to the backup line to achieve quick route switching.

Configuration Conditions

Before configuring BGP to link with BFD, ensure that:

- Enable BGP.
- Configure an IPv6 BGP neighbor and establish a session successfully.

Configure EBGP to Link with BFD

EBGP coordination with BFD is based on the single-hop BFD session. The BFD session parameters shall be configured in the interface mode.

Table 45-46 Configure EBGP to Link with BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure EBGP to link with BFD	**neighbor** { *neighbor-address* | *peer-group-name* } **fall-over bfd** [**single-hop**]	Required By default, the neighbor BFD is disabled
Exit the BGP IPv6 unicast configuration mode	**exit-address-family**	-
Exit the BGP configuration mode	**exit**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the minimum receive interval of BFD session	**bfd min-receive-interval** *milliseconds*	Optional By default, the minimum receive interval of BFD session is 1000s
Configure the minimum send interval of BFD session	**bfd min-transmit-interval** *milliseconds*	Optional By default, the minimum send interval of BFD session is 1000s

Steps	Command	Description
Configure BFD session detection timeout multiplier	**bfd multiplier** *number*	Optional By default, the BFD session detection timeout multiplier is 5

NOTE

- Refer to the Reliability technology - BFD command and BFD configuration sections for relevant BFD configuration.

Configure IBGP to Link with BFD

IBGP coordination with BFD is based on the multi-hop BFD session. The BFD session parameters shall be configured in the BGP mode.

Table 45-47 Configure IBGP to Link with BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the BGP configuration mode	**router bgp** *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	**address-family ipv6 unicast**	-
Configure IBGP to link with BFD	**neighbor** { *neighbor-address* | *peer-group-name* } **fall-over bfd** [**single-hop**]	Required By default, the neighbor BFD is disabled
Configure the minimum receive interval of BFD session	**bfd min-receive-interval** *milliseconds*	Optional By default, the minimum receive interval of BFD session is 1000s
Configure the minimum send interval of BFD session	**bfd min-transmit-interval** *milliseconds*	Optional By default, the minimum send interval

Steps	Command	Description
		of BFD session is 1000s
Configure BFD session detection timeout multiplier	**bfd multiplier** *number*	Optional By default, the BFD session detection timeout multiplier is 5

45.2.9 IPv6 BGP Monitoring and Maintaining *-E -A*

Table 45-48 BGP Monitoring and Maintaining

Command	Description
clear bgp ipv6 { ***** | *as-number* **|** **peer-group** *peer-group-name* **|** **external** | *neighbor-address* } [**vrf** *vrf-name*]	Reset the BGP neighbor
clear bgp [**ipv6 unicast**] **dampening** [*ipv6-address* | *ipv6-address*/*mask-length*]	Clear the dampening route
clear bgp [**ipv6 unicast**] **flap-statistics** [*ipv6-address* | *ipv6-address*/*mask-length*]	Clear the flap statistics
clear bgp [**ipv6]** { * | *as-number* **|** **peer-group** *peer-group-name* **|** **external** | *neighbor-address*} [**vrf** *vrf-name*] { [**soft**] [**in** | **out**] }	Soft-reconfigure the neighbor
clear bgp [**ipv6**] { ***** | *neighbor-address* | *as-number* | **peer-group** *peer-group-name* | **external** } [**vrf** *vrf-name*] **in prefix-filter**	Advertise ORF to the neighbor
show bgp{ipv6 unicast | vpnv6 unicast vrf *vrf-name* } [*ipv6-address* | *ipv6-address*/*mask-length*]	Show the route information under the corresponding address family of BGP
show ip bgp attribute-info	Show the information about public route attributes of BGP

Command	Description
show bgp ipv6 unicast community [*community-number* / *aa:nn* / **exact-match** / **local-AS** / **no-advertise** / **no-export**]	Show the route information that matches the specified community attributes
show bgp ipv6 unicast community-list *community-list-name*	Show the Community list where the route information is applied
show bgp {**ipv6 unicast | vpnv6 unicast vrf** *vrf-name* } **dampening** { **dampened-paths | flap-statistics | parameters** }	Show the detailed information of route dampening
show bgp ipv6 unicast filter-list *filter-list-name* [**exact-match**]	Show the routes that the AS_PATH ACL matches
show bgp ipv6 unicast inconsistent-as	Show conflicting routes of AS_PATH
show bgp { **ipv6 unicast | vpnv6 uicast vrf** *vrf-name* **}** **neighbors** [*ipv6-address*]	Show the detailed information about BGP neighbors
show bgp ipv6 unicast prefix-list *prefix-list-name*	Show the routes that the prefix-list matches
show bgp ipv6 unicast quote-regexp *as-path-list-name*	Show the routes that the AS_PATH list matches
show bgp ipv6 unicast regexp *as-path-list-name*	Show the routes that the AS_PATH list matches
show bgp ipv6 unicast route-map *rtmap-name*	Show the routing that the route map matches
show ip bgp scan	Show BGP scan information
show bgp {**ipv6 unicast | vpnv6 vrf** *vrf-name* } **summary**	Show the information about the neighbor summary of BGP

45.3 IPv6 BGP Typical Configuration Example

45.3.1 Configure Basic Functions of IPv6 BGP *-E -A*

Network Requirements

- Establish EBGP neighbors between Device1 and Device2 and IBGP neighbors between Device2 and Device3.
- Device1 learns the interface direct route 2001:4::/64 from Device3, and Device3 learns the interface direct route 2001:1::/64 from Device1.

Network Topology

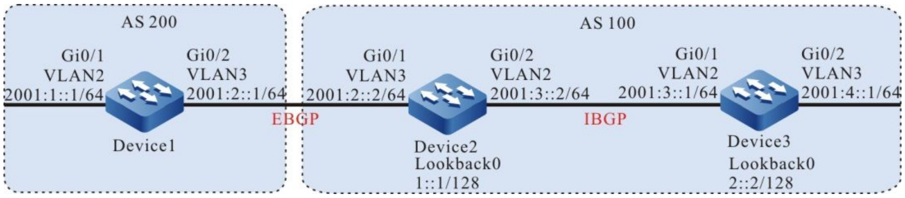


Figure 45-1 Networking for Configuring the Basic Functions of IPv6 BGP

Configuration Steps

Step 1: Configure IPv6 global unicast addresses for the ports. (omitted)

Step 2: Configure OSPFv3 to make the Loopback routes between the devices are mutually reachable.

#Configure Device2.

```
Device2#configure terminal
        Device2(config)#ipv6 router ospf 100
        Device2(config-ospf6)#router-id 2.2.2.2
        Device2(config-ospf6)#exit
        Device2(config)#interface vlan 2
        Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
        Device2(config-if-vlan2)#exit
        Device2(config)#interface loopback 0
        Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
        Device2(config-if-loopback0)#exit
```

#Configure Device3.

```
Device3#configure terminal
        Device3(config)#ipv6 router ospf 100
        Device3(config-ospf6)#router-id 3.3.3.3
        Device3(config-ospf6)#exit
        Device3(config)#interface vlan 2
        Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
```

```
Device3(config-if-vlan2)#exit

Device3(config)#interface loopback 0

Device3(config-if-loopback0)#ipv6 router ospf 100 area 0

Device3(config-if-loopback0)#exit
```

#Query the routing table of Device2.

```
Device2#show ipv6 route

Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS

      U - Per-user Static route

      O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]

    via ::, 1w1d:11:51:37 PM, lo0

LC  1::1/128 [0/0]

    via ::, 12:09:34 AM, loopback0

O   2::2/128 [110/2]

    via fe80::201:7aff:fec0:525a, 00:05:29, vlan2

C   2001:2::/64 [0/0]

    via ::, 12:09:41 AM, vlan3

L   2001:2::2/128 [0/0]

    via ::, 12:09:39 AM, vlan3

C   2001:3::/64 [0/0]

    via ::, 12:08:55 AM, vlan2

L   2001:3::2/128 [0/0]

    via ::, 12:08:53 AM, vlan2
```

#Query the routing table of Device3.

```
Device3#show ipv6 route

Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS

      U - Per-user Static route

      O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]

    via ::, 1w5d:6:34:53 PM, lo0

O   1::1/128 [110/2]

    via fe80::201:7aff:fe5e:6d2e, 12:29:59 AM, vlan2

LC  2::2/128 [0/0]

    via ::, 12:32:36 AM, loopback0

C   2001:3::/64 [0/0]
```

```
    via ::, 12:32:59 AM, vlan2
L   2001:3::1/128 [0/0]
    via ::, 12:32:58 AM, vlan2
C   2001:4::/64 [0/0]
    via ::, 12:32:44 AM, vlan3
L   2001:4::1/128 [0/0]
    via ::, 12:32:43 AM, vlan3
```

As you can see, Device2 and Device3 have learned the peer Loopback routes by running the OSPFv3 protocol to prepare for establishing IBGP neighbors through the Loopback in the next step.

Step 3: Configure basic functions of IPv6 BGP.

#Configure Device1.

Configure an EBGP peer that establishes direct connection with Device2 and introduce 2001:1::/64 to BGP through network.

```
Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 100
Device1(config-bgp-af)#network 2001:1::/64
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#Configure Device2.

Configure an EBGP peer that establishes direct connection with Device1, configure an IBGP peer that establishes non-direct connection with Device3 through Loopback0, and set the next hop of the advertisement route to itself

```
Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:2::1 remote-as 200
Device2(config-bgp-af)#neighbor 2::2 remote-as 100
Device2(config-bgp-af)#neighbor 2::2 next-hop-self
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 2::2 update-source loopback 0
Device2(config-bgp)#exit
```

#Configure Device3.

Establish non-direct IBGP peer relationship with Device2 through Loopback0 and introduce 2001:4::/64 to BGP through network.

```
Device3(config)#router bgp 100
Device3(config-bgp)#bgp router-id 3.3.3.3
```

```
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 1::1 remote-as 100
Device3(config-bgp-af)#network 2001:4::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 1::1 update-source loopback 0
Device3(config-bgp)#exit
```

NOTE

- To prevent route oscillations, all IBGP neighbors are established through the Loopbacks, and OSPFv3 is required to synchronize the route information of the Loopbacks between IBGP neighbors.

Step 4: Check the result.

# Query the IPv6 BGP neighbor state on Device2.

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor       V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2::2           4   100       8       6        3    0    0 00:04:12        1
2001:2::1      4   200      15      15        3    0    0 00:11:17        1

Total number of neighbors 2
```

It can be seen from the numbers (number of prefixes of routes received from the neighbors) in the column State/PfxRcd that Device2 has successfully established IPv6 BGP neighbors with Device1 and Device3.

#Query the routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
     via ::, 1w2d:12:42:57 AM, lo0
```

```
C   2001:1::/64 [0/0]
    via ::, 12:02:59 AM, vlan2
L   2001:1::1/128 [0/0]
    via ::, 12:02:56 AM, vlan2
C   2001:2::/64 [0/0]
    via ::, 12:52:17 AM, vlan3
L   2001:2::1/128 [0/0]
    via ::, 12:52:16 AM, vlan3
B   2001:4::/64 [20/0]
    via 2001:2::2, 00:06:13, vlan3
```

#Query the routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
      U - Per-user Static route
      O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
    via ::, 1w2d:12:34:53 AM, lo0
LC  1::1/128 [0/0]
    via ::, 12:52:49 AM, loopback0
O   2::2/128 [110/2]
    via fe80::201:7aff:fec0:525a, 12:48:45 AM, vlan2
B   2001:1::/64 [20/0]
    via 2001:2::1, 12:03:18 AM, vlan3
C   2001:2::/64 [0/0]
    via ::, 12:52:57 AM, vlan3
L   2001:2::2/128 [0/0]
    via ::, 12:52:55 AM, vlan3
C   2001:3::/64 [0/0]
    via ::, 12:52:10 AM, vlan2
L   2001:3::2/128 [0/0]
    via ::, 12:52:09 AM, lo0
B   2001:4::/64 [200/0]
    via 2::2, 00:07:27, vlan2
```

#Query the routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
      U - Per-user Static route
      O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
    via ::, 1w5d:6:54:38 PM, lo0
O   1::1/128 [110/2]
    via fe80::201:7aff:fe5e:6d2e, 12:49:44 AM, vlan2
LC  2::2/128 [0/0]
    via ::, 12:52:21 AM, loopback0
B   2001:1::/64 [200/0]
    via 1::1, 12:03:54 AM, vlan2
C   2001:3::/64 [0/0]
    via ::, 12:52:44 AM, vlan2
L   2001:3::1/128 [0/0]
    via ::, 12:52:43 AM, vlan2
C   2001:4::/64 [0/0]
    via ::, 12:52:29 AM, vlan3
L   2001:4::1/128 [0/0]
    via ::, 12:52:28 AM, vlan3
```

As you can see, Device1 learns the interface direct route 2001:4::/64 from Device3, and Device3 learns the interface direct route 2001:1::/64 from Device1.

45.3.2 Configure IPv6 BGP Route Re-distribution *-E -A*

Network Requirements

- Establish an OSPFv3 neighbor between Device3 and Device2 and advertise the interface direct route 2001:3::/64 to Device2.
- Establish EBGP neighbors between Device1 and Device2. Device2 Re-distributes the learned OSPFv3 route to IPv6 BGP and advertises to Device1.

Network Topology

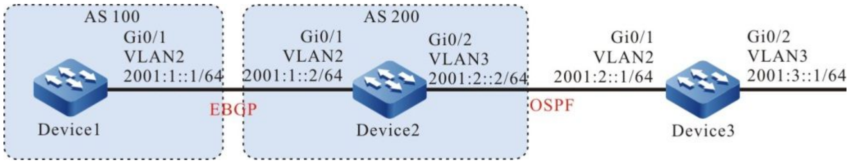


Figure 45-2 Networking for Configuring IPv6 BGP to Re-distribute Routes

Configuration Steps

Step 1: Configure IPv6 global unicast addresses for the ports. (omitted)

Step 2: Configure OSPFv3, so that Device2 learns the direct interface route 2001:3::/64 of Device3.

#Configure Device2.

```
Device2#configure terminal
            Device2(config)#ipv6 router ospf 100
            Device2(config-ospf6)#router-id 2.2.2.2
            Device2(config-ospf6)#exit
            Device2(config)#interface vlan 3
            Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
            Device2(config-if-vlan3)#exit
```

#Configure Device3.

```
Device3#configure terminal
            Device3(config)#ipv6 router ospf 100
            Device3(config-ospf6)#router-id 3.3.3.3
            Device3(config-ospf6)#exit
            Device3(config)#interface vlan 2
            Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
            Device3(config-if-vlan2)#exit
            Device3(config)#interface vlan 3
            Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
            Device3(config-if-vlan3)#exit
```

#Query the routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
   U - Per-user Static route
   O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w2d:1:10:38 AM, lo0
C   2001:1::/64 [0/0]
    via ::, 12:06:25 AM, vlan2
L   2001:1::2/128 [0/0]
    via ::, 12:06:24 AM, vlan2
C   2001:2::/64 [0/0]
    via ::, 12:05:46 AM, vlan3
L   2001:2::2/128 [0/0]
    via ::, 12:05:43 AM, vlan3
O   2001:3::/64 [110/2]
    via fe80::201:7aff:fec0:525a, 12:02:41 AM, vlan3
```

According to the routing table, Device2 has learned the OSPFv3 route 2001:3::/64 advertised by Device3.

Step 3: Configure basic functions of IPv6 BGP.

#Configure Device1.

```
Device1#configure terminal
                    Device1(config)#router bgp 100
                    Device1(config-bgp)#bgp router-id 1.1.1.1
                    Device1(config-bgp)#address-family ipv6
                    Device1(config-bgp-af)#neighbor 2001:1::2 remote-as 200
                    Device1(config-bgp-af)#exit-address-family
                    Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

# Query the IPv6 BGP neighbor state on Device2.

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::1       4   100       2       2        1    0    0 00:00:50        0

Total number of neighbors 1
```

As you can see, Device2 has successfully established an IPv6 BGP neighbor with Device1.

Step 4: Configure IPv6 BGP to Re-distribute OSPFv3 routes.

#Configure Device2.

```
Device2(config)#router bgp 200
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#redistribute ospf 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

Step 5: Check the result.

#Query the IPv6 BGP routing table of Device2.

```
Device2#show bgp ipv6 unicast
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
         S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network           Next Hop          Metric     LocPrf Weight Path
[O]*> 2001:2::/64        ::                  1          32768 ?
[O]*> 2001:3::/64        ::                  2          32768 ?
```

As you can see, the OSPFv3 routes have been successfully Re-distributed to IPv6 BGP.

#Query the routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
         S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network           Next Hop          Metric     LocPrf Weight Path
[B]*> 2001:2::/64       2001:1::2            1              0 200 ?
[B]*> 2001:3::/64       2001:1::2            2              0 200 ?
```

As you can see, Device1 has successfully learned the routes 2001:2::/64 and 2001:3::/64.

NOTE

- In an actual application, if there are two or more AS border devices, it is recommended that you do not Re-distribute routes between different routing protocols. If route Re-distribution must be configured, you are required to configure route control policies such as route filtration and filtration summary on the AS border devices to prevent routing loops.

45.3.3 Configure IPv6 BGP Community Attributes *-E -A*

Network Requirements

- Establish EBGP neighbors between Device1 and Device2.
- Device1 introduces two direct routes 2001:1::/64 and 2001:2::/64 to BGP through network and sets different community attributes to two routes when advertising to Device2.
- When receiving the routes advertised by Device1, Device2 filters the route 2001:1::/64 and allows the route 2001:2::/64 by matching the community attributes in the incoming direction of the neighbor.

Network Topology

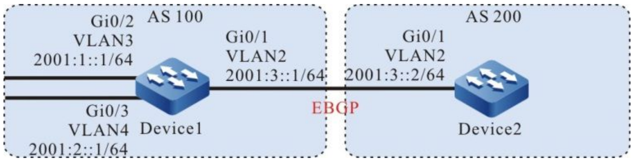


Figure 45-3 Networking for Configuring IPv6 BGP Community Attributes

Configuration Steps

Step 1: Configure IPv6 global unicast addresses for the ports. (omitted)

Step 2: Configure basic functions of IPv6 BGP.

#Configure Device1.

```
Device1#configure terminal
                Device1(config)#router bgp 100
                Device1(config-bgp)#bgp router-id 1.1.1.1
                Device1(config-bgp)#address-family ipv6
                Device1(config-bgp-af)#neighbor 2001:3::2 remote-as 200
                Device1(config-bgp-af)#network 2001:1::/64
                Device1(config-bgp-af)#network 2001:2::/64
                Device1(config-bgp-af)#exit-address-family
                Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2#configure terminal
                Device2(config)#router bgp 200
                Device2(config-bgp)#bgp router-id 2.2.2.2
                Device2(config-bgp)#address-family ipv6
                Device2(config-bgp-af)#neighbor 2001:3::1 remote-as 100
                Device2(config-bgp-af)#exit-address-family
                Device2(config-bgp)#exit
```

# Query the IPv6 BGP neighbor state on Device1.

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor       V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:3::2      4   200       3       4        1    0    0 12:01:02 AM       0
```

```
Total number of neighbors 1
```

As you can see, Device1 has successfully established an IPv6 BGP neighbor with Device2.

#Query the routing table on Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w2d:5:45:34 AM, lo0
B   2001:1::/64 [20/0]
    via 2001:3::1, 12:01:35 AM, vlan2
B   2001:2::/64 [20/0]
    via 2001:3::1, 12:01:35 AM, vlan2
C   2001:3::/64 [0/0]
    via ::, 12:04:09 AM, vlan2
L   2001:3::2/128 [0/0]
    via ::, 12:04:08 AM, vlan2
```

As you can see, Device2 has successfully learned the routes 2001:1::/64 and 2001:2::/64.

Step 3: Configure an ACL and route policy and set IPv6 BGP community attributes.

#Configure Device1.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 2001:1::/64 any
Device1(config-v6-list)#exit
Device1(config)#ipv6 access-list extended 7002
Device1(config-v6-list)#permit ipv6 2001:2::/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map CommunitySet 10
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set community 100:1
Device1(config-route-map)#exit
Device1(config)#route-map CommunitySet 20
Device1(config-route-map)#match ipv6 address 7002
Device1(config-route-map)#set community 100:2
Device1(config-route-map)#exit
```

Set different community attributes to the routes 2001:1::/64 and 2001:2::/64 by configuring an ACL and route policy.

Step 4: Configure route policy for IPv6 BGP.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:3::2 route-map CommunitySet out
Device1(config-bgp-af)#neighbor 2001:3::2 send-community
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#Query the IPv6 BGP routing table of Device2.

```
Device2#show bgp ipv6 unicast 2001:1::/64
BGP routing table entry for 2001:1::/64
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  100
    2001:3::1 (metric 10) from 2001:3::1 (1.1.1.1)



     Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 100:1
      Last update: 12:00:24 AM ago
Device2#show bgp ipv6 unicast 2001:2::/64
BGP routing table entry for 2001:2::/64
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  100
    2001:3::1 (metric 10) from 2001:3::1 (1.1.1.1)



     Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 100:2
      Last update: 12:00:30 AM ago
```

According to IPv6 BGP routing table of Device2, the community attribute of the route 2001:1::/64 is set to 100: 1 and of 2001:2::/64 is set to 100: 2.

Step 5: Configure IPv6 BGP route filtration.

#Configure Device2.

```
Device2(config)#ip community-list 1 permit 100:2
Device2(config)#route-map CommunityFilter
Device2(config-route-map)#match community 1
```

```
Device2(config-route-map)#exit
Device2(config)#router bgp 200
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:3::1 route-map CommunityFilter in
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

Step 6: Check the result.

#Query the routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
     via ::, 1w2d:5:58:57 AM, lo0
B   2001:2::/64 [20/0]
     via 2001:3::1, 12:00:05 AM, vlan2
C   2001:3::/64 [0/0]
     via ::, 12:17:32 AM, vlan2
L   2001:3::2/128 [0/0]
     via ::, 12:17:30 AM, vlan2
```

According to IPv6 BGP routing table of Device2, the route 2001:1::/64 is filtered in the incoming direction and the route 2001:2::/64 is allowed.

NOTE

- The route policy configured on the IPv6 BGP neighbor may take effect only after IPv6 BGP neighbor is re-configured.
- The community attributes can be advertised to the peer only after the command **send-community** is configured.

45.3.4 Configure IPv6 BGP Route Reflector *-E -A*

Network Requirements

- Establish EBGP neighbors between Device3 and Device4. Device4 advertises the route 2001:4::/64 to Device3.
- Device2 establishes IBGP neighbors with Device3 and Device1 respectively.

Configure a route reflector on Device2, with Device1 and Device3 as the clients, so that Device1 can learn the route 2001:4::/64 advertised by Device4.

Network Topology

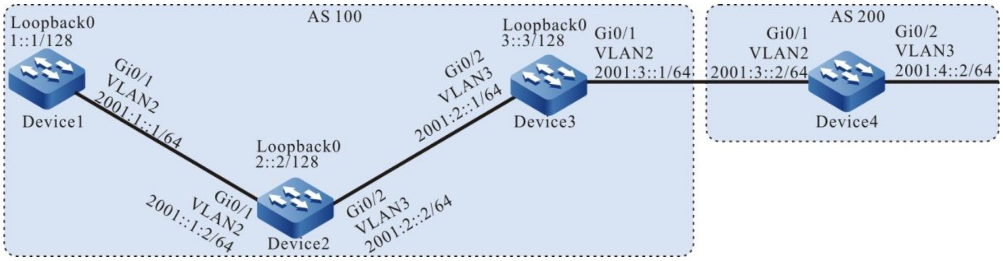


Figure 45-4 Networking for Configuring IPv6 BGP Route Reflector

Configuration Steps

Step 1: Configure IPv6 global unicast addresses for the ports. (omitted)

Step 2: Configure OSPFv3 to make the Loopback routes between the devices are mutually reachable.

#Configure Device1.

```
Device1#configure terminal
                Device1(config)#ipv6 router ospf 100
                Device1(config-ospf6)#router-id 1.1.1.1
                Device1(config-ospf6)#exit
                Device1(config)#interface vlan 2
                Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
                Device1(config-if-vlan2)#exit
                Device1(config)#interface loopback 0
                Device1(config-if-loopback0)#ipv6 router ospf 100 area 0
                Device1(config-if-loopback0)#exit
```

#Configure Device2.

```
Device2#configure terminal
                Device2(config)#ipv6 router ospf 100
                Device2(config-ospf6)#router-id 2.2.2.2
                Device2(config-ospf6)#exit
                Device2(config)#interface vlan 2
                Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
                Device2(config-if-vlan2)#exit
                Device2(config)#interface vlan 3
                Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
                Device2(config-if-vlan3)#exit
                Device2(config)#interface loopback 0
                Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
```

```
Device2(config-if-loopback0)#exit
```

#Configure Device3.

```
Device3#configure terminal
        Device3(config)#ipv6 router ospf 100
        Device3(config-ospf6)#router-id 3.3.3.3
        Device3(config-ospf6)#exit
        Device3(config)#interface vlan 3
        Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
        Device3(config-if-vlan3)#exit
        Device3(config)#interface loopback 0
        Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
        Device3(config-if-loopback0)#exit
```

#Query the routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
   via ::, 1w2d:6:26:16 AM, lo0
LC  1::1/128 [0/0]
   via ::, 12:13:56 AM, loopback0
O   2::2/128 [110/2]
   via fe80::201:7aff:fec0:525a, 12:09:06 AM, vlan2
O   3::3/128 [110/3]
   via fe80::201:7aff:fec0:525a, 12:00:36 AM, vlan2
C   2001:1::/64 [0/0]
   via ::, 12:14:03 AM, vlan2
L   2001:1::1/128 [0/0]
   via ::, 12:14:02 AM, vlan2
O   2001:2::/64 [110/2]
   via fe80::201:7aff:fec0:525a, 12:09:06 AM, vlan2
```

#Query the routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
    via ::, 1w6d:12:46:09 AM, lo0
O   1::1/128 [110/2]
    via fe80::201:7aff:fe5e:6d2e, 12:10:05 AM, vlan2
LC  2::2/128 [0/0]
    via ::, 12:14:23 AM, loopback0
O   3::3/128 [110/2]
    via fe80::201:7aff:fe62:bb80, 12:01:44 AM, vlan3
C   2001:1::/64 [0/0]
    via ::, 12:14:48 AM, vlan2
L   2001:1::2/128 [0/0]
    via ::, 12:14:47 AM, vlan2
C   2001:2::/64 [0/0]
    via ::, 12:14:41 AM, vlan3
L   2001:2::2/128 [0/0]
    via ::, 12:14:39 AM, vlan3
```

#Query the routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w2d:6:37:24 AM, lo0
O   1::1/128 [110/3]
    via fe80::201:7aff:fec0:525b, 12:02:39 AM, vlan3
O   2::2/128 [110/2]
    via fe80::201:7aff:fec0:525b, 12:02:39 AM, vlan3
LC  3::3/128 [0/0]
    via ::, 12:14:45 AM, loopback0
O   2001:1::/64 [110/2]
    via fe80::201:7aff:fec0:525b, 12:02:39 AM, vlan3
C   2001:2::/64 [0/0]
    via ::, 12:15:03 AM, vlan3
L   2001:2::1/128 [0/0]
    via ::, 12:15:02 AM, vlan3
C   2001:3::/64 [0/0]
    via ::, 12:14:55 AM, vlan2
L   2001:3::1/128 [0/0]
```

```
via ::, 12:14:54 AM, vlan2
```

As you can see, Device1, Device2 and Device3 learn each other's loopback interface routes.

Step 3: Configure basic functions of IPv6 BGP.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2::2 remote-as 100
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#neighbor 2::2 update-source loopback 0
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 remote-as 100
Device2(config-bgp-af)#neighbor 3::3 remote-as 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 1::1 update-source loopback 0
Device2(config-bgp)#neighbor 3::3 update-source loopback 0
Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 2::2 remote-as 100
Device3(config-bgp-af)#neighbor 2::2 next-hop-self
Device3(config-bgp-af)#neighbor 2001:3::2 remote-as 200
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 2::2 update-source loopback 0
Device3(config-bgp)#exit
```

#Configure Device4.

```
Device4#configure terminal
    Device4(config)#router bgp 200
    Device4(config-bgp)#bgp router-id 4.4.4.4
    Device4(config-bgp)#address-family ipv6
    Device4(config-bgp-af)#neighbor 2001:3::1 remote-as 100
    Device4(config-bgp-af)#network 2001:4::/64
```

```
Device4(config-bgp-af)#exit-address-family
Device4(config-bgp)#exit
```

# Query the IPv6 BGP neighbor state on Device2.

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1::1            4   100      10      10        2    0    0 00:07:18        0
3::3            4   100      10       9        2    0    0 00:06:53        1

Total number of neighbors 2
```

#Query the IPv6 BGP neighbor state on Device4.

```
Device4#show bgp ipv6 unicast summary
BGP router identifier 4.4.4.4, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:3::1       4   100       3       4        2    0    0 12:01:45 AM       0

Total number of neighbors 1
```

As you can see, IPv6 BGP neighbors are established successfully between the devices.

#Query the IPv6 BGP routing table of Device3.

```
Device3#show bgp ipv6 unicast
BGP table version is 3, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network           Next Hop           Metric     LocPrf Weight Path
[B]*> 2001:4::/64        2001:3::2              0              0 200 i
```

#Query the IPv6 BGP routing table of Device2.

```
Device2#show bgp ipv6 unicast
BGP table version is 7, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network            Next Hop            Metric     LocPrf Weight Path
[B]*>i2001:4::/64        3::3                  0        100      0 200 i
```

#Query the IPv6 BGP routing table of Device1.

```
Device1#show bgp ipv6 unicast
```

According to the above results, Device2 and Device3 have learned the route 2001:4::/64, while Device2 does not advertise the route to Device1.

Step 4: Configure IPv6 BGP Route Reflector.

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 route-reflector-client
Device2(config-bgp-af)#neighbor 3::3 route-reflector-client
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

On Device2, configure Device1 and Device3 as the clients of the route reflector.

Step 5: Check the result.

#Query the routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network            Next Hop            Metric     LocPrf Weight Path
[B]*>i2001:4::/64        3::3                  0        100      0 200 i
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
      U - Per-user Static route
      O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w2d:6:48:52 AM, lo0
LC  1::1/128 [0/0]
    via ::, 12:36:32 AM, loopback0
O   2::2/128 [110/2]
    via fe80::201:7aff:fec0:525a, 12:31:42 AM, vlan2
```

```
O   3::3/128 [110/3]
     via fe80::201:7aff:fec0:525a, 12:23:12 AM, vlan2
C   2001:1::/64 [0/0]
     via ::, 12:36:39 AM, vlan2
L   2001:1::1/128 [0/0]
     via ::, 12:36:38 AM, vlan2
O   2001:2::/64 [110/2]
     via fe80::201:7aff:fec0:525a, 12:31:42 AM, vlan2
B   2001:4::/64 [200/0]
     via 3::3, 12:01:16 AM, vlan2
```

In BGP of Device2, configure Device1 and Device3 as the clients of the route reflector. Device2 successfully reflects the route 2001:4::/64 to the client Device1.

NOTE

- When an IPv6 BGP neighbor is configured as the client of the route reflector, the neighbor is re-configured.

45.3.5 Configure IPv6 BGP Route Aggregation *-E -A*

Network Requirements

- Establish an OSPFv3 neighbor between Device1 and Device3. Device3 advertises two routes 2002:1::/64 and 2002:2::/64 to Device1.
- Establish EBGP neighbors between Device1 and Device2.
- On Device1, aggregate 2002:1::/64 and 2002:2::/64 into the route 2002::/30 and advertise to Device2.

Network Topology

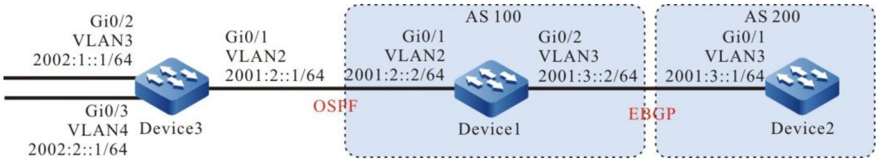


Figure 45-5 Networking for Configuring IPv6 BGP Route Aggregation

Configuration Steps

Step 1: Configure IPv6 global unicast addresses for the ports. (omitted)

Step 2: Configure OSPFv3, so that Device1 can learn two routes 2002:1:/64 and 2002:2::/64 advertised by Device3.

#Configure Device1.

```
Device1#configure terminal
        Device1(config)#ipv6 router ospf 100
        Device1(config-ospf6)#router-id 1.1.1.1
        Device1(config-ospf6)#exit
        Device1(config)#interface vlan 2
        Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
        Device1(config-if-vlan2)#exit
```

#Configure Device3.

```
Device3#configure terminal
        Device3(config)#ipv6 router ospf 100
        Device3(config-ospf6)#router-id 3.3.3.3
        Device3(config-ospf6)#exit
        Device3(config)#interface vlan 2
        Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
        Device3(config-if-vlan2)#exit
        Device3(config)#interface vlan 3
        Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
        Device3(config-if-vlan3)#exit
        Device3(config)#interface vlan 4
        Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
        Device3(config-if-vlan4)#exit
```

#Query the routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
   U - Per-user Static route
   O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w2d:7:35:38 AM, lo0
C   2001:3::/64 [0/0]
    via ::, 12:01:11 AM, vlan3
L   2001:3::2/128 [0/0]
    via ::, 12:01:10 AM, vlan3
C   2001:2::/64 [0/0]
    via ::, 12:01:06 AM, vlan2
L   2001:2::2/128 [0/0]
    via ::, 12:01:04 AM, vlan2
O   2002:1::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 12:01:54 AM, vlan2
```

```
O   2002:2::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 12:01:54 AM, vlan2
```

As you can see, Device1 has learned the routes 2002:1:1::/64 and 2002:1:2::/64 advertised by Device3.

Step 3: Configure basic functions of IPv6 BGP.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:3::1 remote-as 200
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2#configure terminal
            Device2(config)#router bgp 200
            Device2(config-bgp)#bgp router-id 2.2.2.2
            Device2(config-bgp)#address-family ipv6
            Device2(config-bgp-af)#neighbor 2001:3::2 remote-as 100
            Device2(config-bgp-af)# xit-address-family
            Device2(config-bgp)#exit
```

# Query the IPv6 BGP neighbor state on Device1.

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:3::1       4   200       3       3        1    0    0 12:01:16 AM       0
```

Device1 has successfully established an IPv6 BGP neighbor with Device2.

Step 4: Configure IPv6 BGP route aggregation.

Here are two solutions to fulfill the network needs:

Solution 1: configure an IPv6 static route to null0 and introduce it to BGP.

#Configure Device1.

```
Device1(config)#ipv6 route 2002::/30 null 0
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
```

```
Device1(config-bgp-af)#network 2002::/30
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

Check the result.

#Query the IPv6 BGP routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
[B]*> 2002::/30        ::                  0          32768 i
```

As you can see, the aggregate route 2002::/30 has been generated in the IPv6 BGP routing table of Device1.

#Query the routing table of Device2.

```
Device2#show bgp ipv6 unicast
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
[B]*> 2002::/30        2001:3::2           0             0 100 i
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w6d:3:14:01 AM, lo0
C   2001:3::/64 [0/0]
    via ::, 1:20:21 AM, vlan3
L   2001:3::1/128 [0/0]
    via ::, 1:20:20 AM, vlan3
B   2002::/30 [20/0]
    via 2001:3::2, 12:00:44 AM, vlan3
```

As you can see, Device2 has successfully learned the aggregate route 2002::/30 advertised by Device1.

Solution 2: introduce the detailed routes to BGP and then aggregate the routes through the command aggregate-address.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#redistribute ospf 100
Device1(config-bgp-af)#aggregate-address 2002::/30 summary-only
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

Check the result.

#Query the IPv6 BGP routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
[O]*> 2001:2::/64        ::                 1            32768 ?
[B]*> 2002::/30         ::                              32768 i
[O]s> 2002:1::/64        ::                 2            32768 ?
[O]s> 2002:2::/64        ::                 2            32768 ?
```

As you can see, the aggregate route 2002::/30 has been generated in the IPv6 BGP routing table of Device1.

#Query the routing table of Device2.

```
Device2#show bgp ipv6 unicast
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric     LocPrf Weight Path
[B]*> 2001:2::/64       2001:3::2           1             0 100 ?
[B]*> 2002::/30        2001:3::2           0             0 100 i
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w6d:3:16:42 AM, lo0
B   2001:2::/64 [20/0]
    via 2001:3::2, 12:00:50 AM, vlan3
```

```
C   2001:3::/64 [0/0]

     via ::, 1:23:01 AM, vlan3

L   2001:3::1/128 [0/0]

     via ::, 1:23:00 AM, vlan3

B   2002::/30 [20/0]

     via 2001:3::2, 12:00:50 AM, vlan3
```

As you can see, Device2 has successfully learned the aggregate route 2002::/30 advertised by Device1.

NOTE

- In using the aggregate-address command for route aggregation, if you configure the extended command summary-only, the device will only advertise the aggregate route; otherwise, it will advertise the detailed routes and aggregate route simultaneously.

45.3.6 Configure IPv6 BGP Route Preference *-E -A*

Network Requirements

- Device1 establishes IBGP neighbors with Device2 and Device3 respectively and Device4 establishes EBGP neighbors with Device2 and Device3 respectively.
- Device1 advertises two routes 2001:1::/64 and 2001:2::/64 to Device4; Device4 advertises two routes 2001:7::/64 and 2001:8::/64 to Device1.
- By modifying the Local-preference attribute of the routes on Device2 and Device3, Device1 prefers the route 2001:7::/64 advertised by Device3 and the route 2001:8::/64 advertised by Device2.
- By modifying the MED attribute of the routes on Device2 and Device3, Device4 prefers the route 2001:1::/64 advertised by Device3 and the route 2001:2::/64 advertised by Device2.

Network Topology

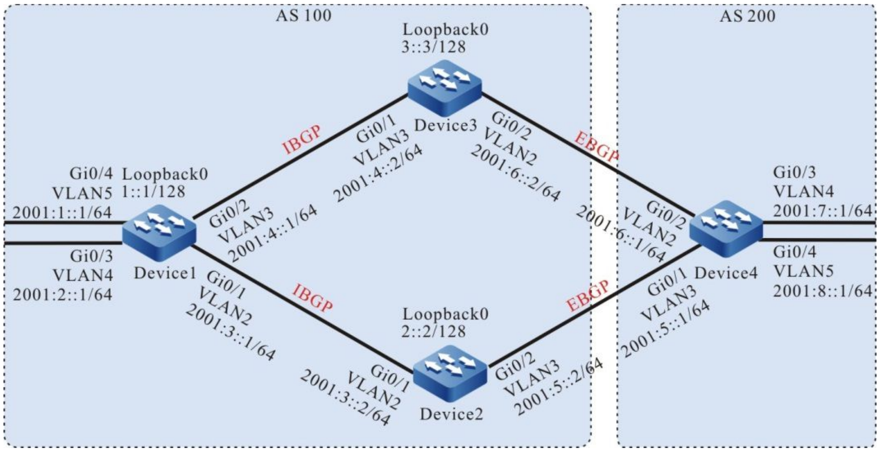


Figure 45-6 Networking for IPv6 BGP Route Preference

Configuration Steps

Step 1: Configure IPv6 global unicast addresses for the ports. (omitted)

Step 2: Configure OSPFv3 to make the Loopback routes between the devices are mutually reachable.

#Configure Device1.

```
Device1#configure terminal
                Device1(config)#ipv6 router ospf 100
                Device1(config-ospf6)#router-id 1.1.1.1
                Device1(config-ospf6)#exit
                Device1(config)#interface vlan 2
                Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
                Device1(config-if-vlan2)#exit
                Device1(config)#interface vlan 3
                Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
                Device1(config-if-vlan3)#exit
                Device1(config)#interface loopback 0
                Device1(config-if-loopback0)#ipv6 router ospf 100 area 0
                Device1(config-if-loopback0)#exit
```

#Configure Device2.

```
Device2#configure terminal
                Device2(config)#ipv6 router ospf 100
                Device2(config-ospf6)#router-id 2.2.2.2
                Device2(config-ospf6)#exit
                Device2(config)#interface vlan 2
                Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
                Device2(config-if-vlan2)#exit
                Device2(config)#interface loopback 0
                Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
                Device2(config-if-loopback0)#exit
```

#Configure Device3.

```
Device3#configure terminal
                Device3(config)#ipv6 router ospf 100
                Device3(config-ospf6)#router-id 3.3.3.3
                Device3(config-ospf6)#exit
                Device3(config)#interface vlan 3
                Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
                Device3(config-if-vlan3)#exit
                Device3(config)#interface loopback 0
```

```
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit
```

#Query the routing table of Device1.

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w5d:4:03:11 AM, lo0
LC  1::1/128 [0/0]
    via ::, 12:08:39 AM, loopback0
O   2::2/128 [110/2]
    via fe80::201:7aff:fe5e:87da, 12:02:04 AM, vlan2
O   3::3/128 [110/2]
    via fe80::201:7aff:fec0:525b, 12:00:38 AM, vlan3
C   2001:1::/64 [0/0]
    via ::, 12:09:12 AM, vlan5
L   2001:1::1/128 [0/0]
    via ::, 12:09:11 AM, vlan5
C   2001:2::/64 [0/0]
    via ::, 12:08:26 AM, vlan4
L   2001:2::1/128 [0/0]
    via ::, 12:08:26 AM, vlan4
C   2001:3::/64 [0/0]
    via ::, 12:09:01 AM, vlan2
L   2001:3::1/128 [0/0]
    via ::, 12:09:00 AM, vlan2
C   2001:4::/64 [0/0]
    via ::, 12:08:55 AM, vlan3
L   2001:4::1/128 [0/0]
    via ::, 12:08:53 AM, vlan3
```

#Query the routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]

     via ::, 2w4d:11:16:51 PM, lo0

O   1::1/128 [110/2]

     via fe80::201:7aff:fe62:bb7f, 12:04:25 AM, vlan2

LC  2::2/128 [0/0]

     via ::, 12:09:31 AM, loopback0

O   3::3/128 [110/3]

     via fe80::201:7aff:fe62:bb7f, 12:02:52 AM, vlan2

C   2001:3::/64 [0/0]

     via ::, 12:09:49 AM, vlan2

L   2001:3::2/128 [0/0]

     via ::, 12:09:48 AM, vlan2

O   2001:4::/64 [110/2]

     via fe80::201:7aff:fe62:bb7f, 12:04:25 AM, vlan2

C   2001:5::/64 [0/0]

     via ::, 12:09:39 AM, vlan3

L   2001:5::2/128 [0/0]

     via ::, 12:09:38 AM, vlan3
```

#Query the routing table of Device3.

```
Device3#show ipv6 route

Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS

       U - Per-user Static route

       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]

     via ::, 2w1d:10:16:55 PM, lo0

O   1::1/128 [110/2]

     via fe80::201:7aff:fe62:bb80, 12:04:27 AM, vlan3

O   2::2/128 [110/3]

     via fe80::201:7aff:fe62:bb80, 12:04:27 AM, vlan3

LC  3::3/128 [0/0]

     via ::, 12:10:48 AM, loopback0

O   2001:3::/64 [110/2]

     via fe80::201:7aff:fe62:bb80, 12:04:27 AM, vlan3

C   2001:4::/64 [0/0]

     via ::, 12:11:55 AM, vlan3

L   2001:4::2/128 [0/0]

     via ::, 12:11:54 AM, vlan3

C   2001:6::/64 [0/0]
```

```
    via ::, 12:11:48 AM, vlan2
L   2001:6::2/128 [0/0]
    via ::, 12:11:47 AM, vlan2
```

As you can see, Device1, Device2 and Device3 learn each other's loopback routes.

Step 3: Configure basic functions of IPv6 BGP.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2::2 remote-as 100
Device1(config-bgp-af)#neighbor 3::3 remote-as 100
Device1(config-bgp-af)#network 2001:1::/64
Device1(config-bgp-af)#network 2001:2::/64
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#neighbor 2::2 update-source loopback 0
Device1(config-bgp)#neighbor 3::3 update-source loopback 0
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 remote-as 100
Device2(config-bgp-af)#neighbor 1::1 next-hop-self
Device2(config-bgp-af)#neighbor 2001:5::1 remote-as 200
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 1::1 update-source loopback 0
Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 1::1 remote-as 100
Device3(config-bgp-af)#neighbor 1::1 next-hop-self
Device3(config-bgp-af)#neighbor 2001:6::1 remote-as 200
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 1::1 update-source loopback 0
Device3(config-bgp)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#bgp router-id 4.4.4.4
Device4(config-bgp)#address-family ipv6
Device4(config-bgp-af)#neighbor 2001:5::2 remote-as 100
Device4(config-bgp-af)#neighbor 2001:6::2 remote-as 100
Device4(config-bgp-af)#network 2001:7::/64
Device4(config-bgp-af)#network 2001:8::/64
Device4(config-bgp-af)#exit-address-family
Device4(config-bgp)#exit
```

# Query the IPv6 BGP neighbor state on Device1.

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2::2            4   100       9      10        4    0    0 00:06:18        2
3::3            4   100       7       8        4    0    0 00:04:29        2

Total number of neighbors 2
```

#Query the IPv6 BGP neighbor state on Device4.

```
Device4#show bgp ipv6 unicast summary
BGP router identifier 4.4.4.4, local AS number 200
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:5::2       4   100       6       5        4    0    0 12:02:43 AM        2
2001:6::2       4   100       5       6        4    0    0 12:02:32 AM        2

Total number of neighbors 2
```

As you can see, Device1 establishes IBGP neighbors successfully with Device2 and Device3 respectively and Device4 establishes EBGP neighbors successfully with Device2 and Device3 respectively.

#Query the routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 1.1.1.1
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network           Next Hop          Metric     LocPrf Weight Path
[B]*> 2001:1::/64         ::                      0            32768 i
[B]*> 2001:2::/64         ::                      0            32768 i
[B]* i2001:7::/64        3::3                     0        100      0 200 i
[B]*>i                   2::2                     0        100      0 200 i
[B]*>i2001:8::/64        2::2                     0        100      0 200 i
[B]* i                   3::3                     0        100      0 200 i

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
      U - Per-user Static route
      O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w5d:4:20:19 AM, lo0
LC  1::1/128 [0/0]
    via ::, 12:25:47 AM, loopback0
O   2::2/128 [110/2]
    via fe80::201:7aff:fe5e:87da, 12:19:12 AM, vlan2
O   3::3/128 [110/2]
    via fe80::201:7aff:fec0:525b, 12:17:46 AM, vlan3
C   2001:1::/64 [0/0]
    via ::, 12:26:20 AM, vlan5
L   2001:1::1/128 [0/0]
    via ::, 12:26:19 AM, vlan5
C   2001:2::/64 [0/0]
    via ::, 12:25:34 AM, vlan4
L   2001:2::1/128 [0/0]
    via ::, 12:25:34 AM, vlan4
C   2001:3::/64 [0/0]
    via ::, 12:26:09 AM, vlan2
L   2001:3::1/128 [0/0]
    via ::, 12:26:08 AM, vlan2
C   2001:4::/64 [0/0]
    via ::, 12:26:03 AM, vlan3
L   2001:4::1/128 [0/0]
```

```
    via ::, 12:26:01 AM, vlan3
B   2001:7::/64 [200/0]
    via 2::2, 12:03:21 AM, vlan2
B   2001:8::/64 [200/0]
    via 2::2, 12:02:57 AM, vlan2
```

As you can see, the routes 2001:7::/64 and 2001:8::/64 on Device1 select Device2 as the optimal next-hop device.

#Query the routing table of Device4.

```
Device4#show bgp ipv6 unicast
BGP table version is 4, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network           Next Hop          Metric     LocPrf Weight Path
[B]*  2001:1::/64        2001:6::2              0              0 100 i
[B]*>                 2001:5::2             0              0 100 i
[B]*  2001:2::/64        2001:6::2              0              0 100 i
[B]*>                 2001:5::2             0              0 100 i
[B]*> 2001:7::/64        ::                   0           32768 i
[B]*> 2001:8::/64        ::                   0           32768 i

Device4#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
      U - Per-user Static route
      O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w5d:4:14:15 AM, lo0
B   2001:1::/64 [20/0]
    via 2001:5::2, 12:06:52 AM, vlan2
B   2001:2::/64 [20/0]
    via 2001:5::2, 12:06:52 AM, vlan2
C   2001:5::/64 [0/0]
    via ::, 12:26:17 AM, vlan3
L   2001:5::1/128 [0/0]
    via ::, 12:26:16 AM, vlan3
C   2001:6::/64 [0/0]
    via ::, 12:26:24 AM, vlan2
L   2001:6::1/128 [0/0]
```

```
    via ::, 12:26:23 AM, vlan2
C   2001:7::/64 [0/0]
    via ::, 12:25:53 AM, vlan4
L   2001:7::1/128 [0/0]
    via ::, 12:25:51 AM, vlan4
C   2001:8::/64 [0/0]
    via ::, 12:25:40 AM, vlan5
L   2001:8::1/128 [0/0]
    via ::, 12:25:40 AM, vlan5
```

As you can see, the routes 2001:1::/64 and 2001:2::/64 on Device4 select Device3 as the optimal next-hop device.

Step 4: Configure an ACL and route policy and set local-preference and metric.

#Configure Device2.

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-v6-list)#permit ipv6 2001:8::/64 any
Device2(config-v6-list)#exit
Device2(config)#ipv6 access-list extended 7002
Device2(config-v6-list)#permit ipv6 2001:1::/64 any
Device2(config-v6-list)#exit
Device2(config)#route-map SetPriority1 10
Device2(config-route-map)#match ipv6 address 7001
Device2(config-route-map)#set local-preference 110
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority1 20
Device2(config-route-map)#set local-preference 20
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 10
Device2(config-route-map)#match ipv6 address 7002
Device2(config-route-map)#set metric 100
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 20
Device2(config-route-map)#set metric 20
Device2(config-route-map)#exit
```

Configure a route policy on Device2 to set the local-preference of the route 2001:8::/64 to 110 and the metric of the route 2001:1::/64 to 100.

#Configure Device3.

```
Device3(config)#ipv6 access-list extended 7001
Device3(config-v6-list)#permit ipv6 2001:7::/64 any
Device3(config-v6-list)#exit
```

```
Device3(config)#ipv6 access-list extended 7002
Device3(config-v6-list)#permit ipv6 2001:2::/64 any
Device3(config-v6-list)#exit
Device3(config)#route-map SetPriority1 10
Device3(config-route-map)#match ipv6 address 7001
Device3(config-route-map)#set local-preference 110
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority1 20
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 10
Device3(config-route-map)#match ipv6 address 7002
Device3(config-route-map)#set metric 100
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 20
Device3(config-route-map)#exit
```

Configure a route policy on Device3 to set the local-preference of the route 2001:7::/64 to 110 and the metric of the route 2001:2::/64 to 100.

NOTE

- In configuring a route policy, you can create a filtration rule based on a prefix list or ACL. The prefix list can precisely match routing masks while the ACL cannot match routing masks.

Step 5: Configure route policy for IPv6 BGP.

#Configure Device2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 route-map SetPriority1 out
Device2(config-bgp-af)#neighbor 2001:5::1 route-map SetPriority2 out
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

Modify local-preference of 2001:8::/64 in the outgoing direction configured with the neighbor 1::1 on Device2, and modify metric of 2001:1::/64 in the outgoing direction configured with the neighbor 2001:5::1.

#Configure Device3.

```
Device3(config)#router bgp 100
Device3(config-bgp)#address-family ipv6
```

```
Device3(config-bgp-af)#neighbor 1::1 route-map SetPriority1 out
Device3(config-bgp-af)#neighbor 2001:6::1 route-map SetPriority2 out
Device3(config-bgp-af)# exit-address-family
Device2(config-bgp)#exit
```

Modify local-preference of 2001:7::/64 in the outgoing direction configured with the neighbor 10.0.0.1 on Device3, and modify metric of 2001:2::/64 in the outgoing direction configured with the neighbor 2001:6::1.

The route policy configured on the neighbor may take effect only after the neighbor is re-configured.

Step 6: Check the result.

#Query the routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 9, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
         S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric    LocPrf Weight Path
[B]*> 2001:1::/64       ::                  0          32768 i
[B]*> 2001:2::/64       ::                  0          32768 i
[B]* i2001:7::/64       2::2                 0       100      0 200 i
[B]*>i                 3::3                 0       110      0 200 i
[B]*>i2001:8::/64       2::2                 0       110      0 200 i
[B]* i                 3::3                 0       100      0 200 i

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
    via ::, 1w5d:4:59:59 AM, lo0
LC  1::1/128 [0/0]
    via ::, 1:05:27 AM, loopback0
O   2::2/128 [110/2]
    via fe80::201:7aff:fe5e:87da, 12:58:52 AM, gigabitethernet1
O   3::3/128 [110/2]
    via fe80::201:7aff:fec0:525b, 12:57:26 AM, gigabitethernet2
C   2001:1::/64 [0/0]
    via ::, 1:06:00 AM, gigabitethernet0
```

```
L   2001:1::1/128 [0/0]
    via ::, 1:05:59 AM, lo0
C   2001:2::/64 [0/0]
    via ::, 1:05:14 AM, loopback1
L   2001:2::1/128 [0/0]
    via ::, 1:05:14 AM, loopback1
C   2001:3::/64 [0/0]
    via ::, 1:05:49 AM, gigabitethernet1
L   2001:3::1/128 [0/0]
    via ::, 1:05:48 AM, lo0
C   2001:4::/64 [0/0]
    via ::, 1:05:43 AM, gigabitethernet2
L   2001:4::1/128 [0/0]
    via ::, 1:05:41 AM, lo0
B   2001:7::/64 [200/0]
    via 3::3, 12:09:05 AM, gigabitethernet1
B   2001:8::/64 [200/0]
    via 2::2, 12:04:58 AM, gigabitethernet0
```

As you can see, local-preference of the routes 2001:7::/64 and 2001:8::/64 is modified successfully. Device1 prefers the route 2001:8::/64 advertised by Device2 and the route 2001:7::/64 advertised by Device3.

#Query the routing table of Device4.

```
Device4#show bgp ipv6 unicast
BGP table version is 5, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network           Next Hop          Metric     LocPrf Weight Path
[B]*  2001:1::/64        2001:5::2            100                0 100 i
[B]*>                  2001:6::2             0                0 100 i
[B]*> 2001:2::/64        2001:5::2             0                0 100 i
[B]*                   2001:6::2           100                0 100 i
[B]*> 2001:7::/64        ::                    0           32768 i
[B]*> 2001:8::/64        ::                    0           32768 i

Device4#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
      U - Per-user Static route
      O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
     via ::, 1w5d:4:53:45 AM, lo0
B   2001:1::/64 [20/0]
     via 2001:6::2, 12:12:10 AM, gigabitethernet1
B   2001:2::/64 [20/0]
     via 2001:5::2, 12:07:40 AM, gigabitethernet0
C   2001:5::/64 [0/0]
     via ::, 1:05:47 AM, gigabitethernet0
L   2001:5::1/128 [0/0]
     via ::, 1:05:46 AM, lo0
C   2001:6::/64 [0/0]
     via ::, 1:05:54 AM, gigabitethernet1
L   2001:6::1/128 [0/0]
     via ::, 1:05:52 AM, lo0
C   2001:7::/64 [0/0]
     via ::, 01:05:22, gigabitethernet1/0
L   2001:7::1/128 [0/0]
     via ::, 1:05:21 AM, lo0
C   2001:8::/64 [0/0]
     via ::, 1:05:09 AM, gigabitethernet2
L   2001:8::1/128 [0/0]
     via ::, 1:05:09 AM, gigabitethernet2
```

As you can see, metric of the routes 2001:1::/64 and 2001:2::/64 is modified successfully. Device4 prefers the route 2001:2::/64 advertised by Device2 and the route 2001:1::/64 advertised by Device3.

NOTE

- The route policy may be used in the outgoing direction of route advertisement or in the incoming direction of route receiving.

45.3.7 Configure IPv6 BGP to Link with BFD *-E -A*

Network Requirements

- Device1 establishes EBGP neighbors with Device2 and Device3 respectively, and Device2 establishes an IBGP neighbor with Device3.
- Device1 learns the EBGP route 2001: 3::/64 from Device2 and Device3 simultaneously and Device1 prefers to forward data to the network segment 2001:3::/64 through Device2.

- Configure EBGP on Device1 and Device2 to link with BFD. After a fault occurs on the line between Device1 and Device2, BFD can quickly detect the fault and advertise to BGP. At this point. Device1 chooses to forward data to the network segment 2001:3::/64 through Device3.

Network Topology

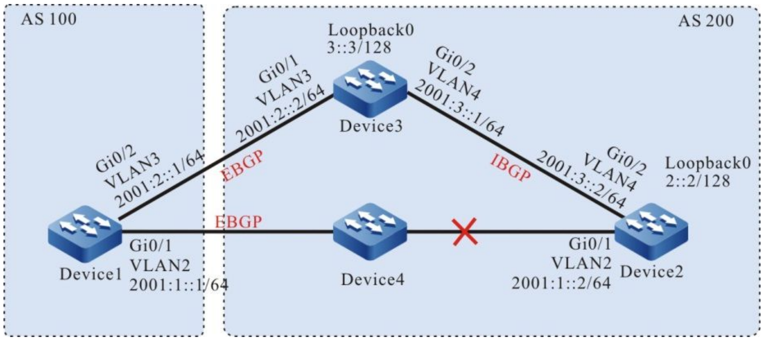


Figure 45-7 Networking for Configuring IPv6 BGP to Link with BFD

Configuration Steps

Step 1: Configure IPv6 global unicast addresses for the ports. (omitted)

Step 2: Configure OSPFv3 to make the Loopback routes between the devices are mutually reachable.

#Configure Device2.

```
Device2#configure terminal
                Device2(config)#ipv6 router ospf 100
                Device2(config-ospf6)#router-id 2.2.2.2
                Device2(config-ospf6)#exit
                Device2(config)# interface vlan 4
                Device2(config-if-vlan4)#ipv6 router ospf 100 area 0
                Device2(config-if-vlan4)#exit
                Device2(config)#interface loopback 0
                Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
                Device2(config-if-loopback0)#exit
```

#Configure Device3.

```
Device3#configure terminal
                Device3(config)#ipv6 router ospf 100
                Device3(config-ospf6)#router-id 3.3.3.3
                Device3(config-ospf6)#exit
                Device3(config)#interface vlan 4
                Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
                Device3(config-if-vlan4)#exit
                Device3(config)# interface loopback 0
                Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
```

```
Device3(config-if-loopback0)#exit
```

#Query the routing table of Device2.

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
     via ::, 1w2d:9:31:22 AM, lo0
LC  2::2/128 [0/0]
     via ::, 12:10:10 AM, loopback0
O   3::3/128 [110/1]
     via fe80::201:7aff:fec0:525a, 12:00:12 AM, vlan4
C   2001:1::/64 [0/0]
     via ::, 12:10:54 AM, vlan2
L   2001:1::2/128 [0/0]
     via ::, 12:10:53 AM, vlan2
C   2001:3::/64 [0/0]
     via ::, 12:10:17 AM, vlan4
L   2001:3::2/128 [0/0]
     via ::, 12:10:16 AM, vlan4
```

#Query the routing table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
     via ::, 1w6d:3:50:38 AM, lo0
O   2::2/128 [110/2]
     via fe80::201:7aff:fe5e:6d2e, 12:02:40 AM, vlan4
LC  3::3/128 [0/0]
     via ::, 12:00:49 AM, loopback0
C   2001:2::/64 [0/0]
     via ::, 12:03:03 AM, vlan3
L   2001:2::2/128 [0/0]
     via ::, 12:03:02 AM, vlan3
C   2001:3::/64 [0/0]
```

```
    via ::, 12:03:18 AM, vlan4
L   2001:3::1/128 [0/0]
    via ::, 12:03:17 AM, vlan4
```

As you can see, Device2 and Device3 learn each other's loopback interface routes.

Step 3: Configure an ACL and route policy and set the route metric.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 2001:3::/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map SetMetric
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set metric 50
Device1(config-route-map)#exit
```

Configure a route policy on Device1 to set the metric of the route 2001:3::/64 to 50.

Step 4: Configure the basic functions of IPv6 BGP and associate a route policy on Device1.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:1::2 remote-as 200
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 200
Device1(config-bgp-af)#neighbor 2001:2::2 route-map SetMetric in
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device2(config-bgp-af)#neighbor 3::3 remote-as 200
Device2(config-bgp-af)#network 2001:3::/64
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 3::3 update-source loopback 0
Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 200
```

```
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 2001:2::1 remote-as 100
Device3(config-bgp-af)#neighbor 2::2 remote-as 200
Device3(config-bgp-af)#network 2001:3::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 2::2 update-source loopback 0
Device3(config-bgp)#exit
```

The route policy configured on the peer may take effect only after the peer is re-configured.

# Query the IPv6 BGP neighbor state on Device1.

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2       4   200       7       6        2    0    0 12:04:00 AM        1
2001:2::2       4   200       5       5        2    0    0 12:02:03 AM        1

Total number of neighbors2
```

# Query the IPv6 BGP neighbor state on Device2.

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3::3          4   200       5       5        2    0    0 12:02:10 AM        1
2001:1::1       4   100       6       7        2    0    0 12:04:38 AM        0

Total number of neighbors 2
```

As you can see, IPv6 BGP neighbors are established successfully among Device1, Device2 and Device3.

#Query the routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network            Next Hop           Metric     LocPrf Weight Path
[B]*  2001:3::/64        2001:2::2              50               0 200 i
[B]*>                  2001:1::2              0                0 200 i



Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
      U - Per-user Static route
      O - OSPF, OE-OSPF External, M - Management



L    ::1/128 [0/0]
     via ::, 1w2d:9:53:27 AM, lo0
C    2001:1::/64 [0/0]
     via ::, 12:24:05 AM, vlan2
L    2001:1::1/128 [0/0]
     via ::, 12:24:02 AM, vlan2
C    2001:2::/64 [0/0]
     via ::, 12:25:21 AM, vlan3
L    2001:2::1/128 [0/0]
     via ::, 12:25:20 AM, vlan3
B    2001:3::/64 [20/0]
     via 2001:1::2, 12:05:06 AM, vlan2
```

As you can see, the route 2001:3::/64 on Device1 selects Device2 as the optimal next-hop device.

Step 5: Configure IPv6 BGP to link with BFD.

#Configure Device1.

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:1::2 fall-over bfd
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#bfd min-transmit-interval 500
Device1(config-if-vlan2)#bfd min-receive-interval 500
Device1(config-if-vlan2)#bfd multiplier 4
Device1(config-if-vlan2)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 200
```

```
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:1::1 fall-over bfd
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#bfd min-transmit-interval 500
Device2(config-if-vlan2)#bfd min-receive-interval 500
Device2(config-if-vlan2)#bfd multiplier 4
Device2(config-if-vlan2)#exit
```

Enable BFD on the EBGP neighbor between Device1 and Device2 and modify BFD to control the minimum send interval, minimum receive interval and detection timeout multiplier of the packets.

Step 6: Check the result.

#Query the BFD session state on Device1.

```
Device1#show bfd session ipv6
OurAddr                  NeighAddr                 State    Holddown   Interface
2001:1::1                2001:1::2                 UP       2000       vlan2
```

As you can see, BFD state on Device1 is correctly up and the holddown time is negotiated as 2000ms.

#When a fault occurs on the line between Device1 and Device2, the route can quickly switch to the backup line.

#Query the routing table of Device1.

```
Device1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop         Metric    LocPrf Weight Path
[B]*> 2001:3::/64      2001:2::2          50              0 200 i
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
    U - Per-user Static route
    O - OSPF, OE-OSPF External, M - Management



L   ::1/128 [0/0]
   via ::, 1w2d:10:06:30 AM, lo0
C   2001:1::/64 [0/0]
   via ::, 12:37:08 AM, vlan2
L   2001:1::1/128 [0/0]
   via ::, 12:37:04 AM, vlan2
```

```
C   2001:2::/64 [0/0]
    via ::, 12:38:24 AM, vlan3
L   2001:2::1/128 [0/0]
    via ::, 12:38:23 AM, vlan3
B   2001:3::/64 [20/0]
    via 2001:2::2, 12:00:16 AM, vlan3
```

As you can see, the next hop of the route 2001 :3 ::/64 is switched to Device3.

46 PBR

46.1 Overview

PBR is a routing mechanism for packet forwarding based on user-customized policies. In routing and forwarding, the packets can be matched according to ACL rules in terms of IP protocol number, source IP address, destination IP address, source TCP/UDP port number, destination TCP/UDP port number, packet priority, TCP flag and other information. The packets meeting the matching conditions are operated according to the specified policies (set the next hop) to complete the packet forwarding control.

Compared with the traditional routing mode of packet forwarding only based on the destination address, PBR is more flexible and can be regarded as an effective supplement and enhancement to the traditional routing mechanism.

46.2 PBR Function Configuration

Table 46-1 PBR Function List

Configuration task	
Configure PBR	Configure the next-hop IP address for packet forwarding
	Configure the next-hop IPv6 address for packet forwarding
	Configure PBR action group bound to ACL
	Configure PBR action group bound to ACL rule
Configure PBR application	Configure ACL with PBR applied to two-layer/three-layer Ethernet interface
	Configure ACL with PBR applied to VLAN

Configuration task	
	Configure ACL with PBR applied to Interface VLAN
	Configure ACL with PBR applied globally

46.2.1 Configure PBR *-S -E -A*

The implementation of PBR relies on the filtering of packets by ACL rule. The ACL rule first filters the out the qualified packets, then performs a PBR on the packets to forward to the next hop.

Configuration Conditions

Before configuring PBR, ensure that:

- Configure ACL and ACL rules.

Configure the Next-Hop IP Address for Packet Forwarding

Configure the next-hop IP address for packet forwarding to specify the destination address of PBR.

At most 6 next-hop IP addresses can be specified for packet forwarding. If multiple next-hop IP addresses are configured at the same time and multiple next-hop IP addresses are reachable, the next hop IP address will be selected for packet forwarding by load balancing.

Table 46-2 Configure the Next-Hop IP Address for Packet Forwarding

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the PBR action group configuration mode	**pbr-action-group** *pbr-action-group-name*	-
Configure the next-hop IP address for packet forwarding	**redirect ipv4-nexthop** *ip-address* [*ip-address*] [*ip-address*] [*ip-address*] [*ip-address*] [*ip-address*]	Required By default, the next-hop IP address for packet forwarding is not configured.

NOTE

- The PBR function does not take effect if all configured next-hop IP addresses for forwarding are unreachable.
- The next-hop IP address cannot be configured as a local IP address, multicast address, or broadcast address.

Configure the Next-Hop IPv6 Address for Packet Forwarding

Configure the next-hop IPv6 address for packet forwarding to specify the destination address of PBR.

At most 6 next-hop IPv6 addresses can be specified for packet forwarding. If multiple next-hop IPv6 addresses are configured at the same time and multiple next-hop IPv6 addresses are reachable, the next hop IPv6 address will be selected for packet forwarding by load balancing.

Table 46-3 Configure the Next-Hop IPv6 Address for Packet Forwarding

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the PBR action group configuration mode	**pbr-action-group** *pb-action-group-name*	-
Configure the next-hop IPv6 address for packet forwarding	**redirect ipv6-nexthop** *ipv6-address* [*ipv6-address*] [*ipv6-address*] [*ipv6-address*] [*ipv6-address*] [*ipv6-address*]	Required By default, the next-hop IPv6 address for packet forwarding is not configured.

NOTE

- The PBR function does not take effect if all configured next-hop IPv6 addresses for forwarding are unreachable.
- The next-hop IPv6 address cannot be configured as a local IPv6 address, multicast address, or broadcast address.

Configure PBR Action Group Bound to ACL

Configure PBR action group bound to ACL and implement the association of all rules in the ACL with the actions executed by PBR.

Once the PBR action group is bound to ACL, all the rules in ACL are associated with actions executed by PBR. As long as the packet received by the port matches the rule in the ACL, the packet is forwarded to the next hop.

Table 46-4 Configure PBR Action Group Bound to ACL

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure PBR action group bound to ACL	**ip pbr-action-group** *pbr-action-group-name* **access-list** { *access-list-number* | *access-list-name* }	Optional By default, no PBR action group is bound to IP ACL. The PBR action group supports IP ACL binding, and IP ACL contains IP standard ACL and IP extended ACL.
	ipv6 pbr-action-group *pbr-action-group-name* **access-list** { *access-list-number* | *access-list-name* }	Optional By default, no PBR action group is bound to IPv6 ACL. The PBR action group supports IPv6 ACL binding, and IPv6 ACL contains IPv6 standard ACL and IPv6 extended ACL.

NOTE

- PBR only takes effect when the configured next-hop IP address is reachable.
- PBR can only take effect against permission rules in ACL.

Configure PBR Action Group Bound to ACL Rule

Configure PBR action group bound to ACL rule and implement the association of ACL rule with the actions executed by PBR.

Once the PBR action group is bound to ACL rule, the ACL rule will be associated with actions executed by PBR. If the packet received by the port matches the ACL rule, it is forwarded according to the next hop specified by the action group.

Table 46-5 Configure PBR Action Group Bound to ACL Rule

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure PBR action group bound to ACL rule	Refer to “Configured IP standard ACL” Refer to “Configure IP extended ACL” Refer to “Configured IPv6 standard ACL” Refer to “Configure IPv6 extended ACL”	In the permission rules for configuring IP standard ACL and extended ACL, PBR action groups must be specified for the PBR to take effect. In the permission rules for configuring IPv6 standard ACL and extended ACL, PBR action groups must be specified for the PBR to take effect.

NOTE

- PBR only takes effect when the configured next-hop IP address is reachable.
- PBR can only take effect against permission rules in ACL.

46.2.2 Configure PBR Application *-S -E -A*

The application of PBR is actually the application of ACL with PBR, and the effectiveness of PBR depends on the ACL rule. ACL may be applied to the two-layer/three-layer Ethernet interface, VLAN, Interface VLAN and globally.

There may be conflicts when ACL with PBR is applied globally, or to VLAN, Interface VLAN and two-layer/three-layer Ethernet interface, respectively. In this case, PBR corresponding to high priority takes effect. The priority is from high to low: port, VLAN/ Interface VLAN and global.

Configuration Conditions

None

Configure ACL with PBR Applied to Two-Layer/Three-Layer Ethernet Interface

After ACL with PBR is applied to two-layer/three-layer Ethernet interface, the corresponding two-layer/three-layer Ethernet interface will have PBR function.

Table 46-6 Configure PBR Applied to Two-Layer/Three-Layer Ethernet Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2/L3 ethernet interface configuration mode	**interface** *interface-name*	Must be chosen alternatively After entering the two-layer/three-layer Ethernet interface configuration mode, the subsequent configuration will only take effect on the current port; after entering the aggregation group configuration mode, the subsequent configuration only takes effect in the aggregation group.
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure PBR applied to port	**ip policy-based-route** { *access-list-number* | *access-list-name* }	Optional By default, IP ACL with PBR is not applied to the port
	ipv6 policy-based-route { *access-list-number* | *access-list-name* }	Optional By default, IPv6 ACL with PBR is not applied to the port

Configure ACL with PBR Applied to VLAN

After ACL with PBR is applied to VLAN, all ports in the corresponding VLAN will have PBR function.

Table 46-7 Configure PBR Applied to VLAN

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter VLAN configuration mode	**vlan** *vlan-id*	-

Steps	Command	Description
Configure PBR applied to VLAN	**ip policy-based-route**{ *access-list-number* | *access-list-name* }	Optional By default, IP ACL with PBR is not applied to VLAN

Configure ACL with PBR Applied to Interface VLAN

After ACL with PBR is applied to the Interface VLAN, the corresponding Interface VLAN will have PBR function.

Table 46-8 Configure PBR Applied to Interface VLAN

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the Interface VLAN configuration mode	**Interface vlan** *vlan-id*	-
Configure PBR applied to Interface VLAN	**ip policy-based-route** { *access-list-number* | *access-list-name* }	Optional By default, IP ACL with PBR is not applied to Interface VLAN
	ipv6 policy-based-route { *access-list-number* | *access-list-name* }	Optional By default, IPv6 ACL with PBR is not applied to Interface VLAN

Configure ACL with PBR Applied Globally

After ACL with PBR is applied globally, all ports of the device will have PBR function.

Table 46-9 Configure PBR Applied Globally

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Configure PBR applied globally	**global ip policy-based-route** { *access-list-number* | *access-list-name* }	Required By default, ACL with PBR is not applied globally

46.2.3 PBR Monitoring and Maintaining ***-S -E -A***

Table 46-10 PBR Monitoring and Maintaining

Command	Description
show pbr-action-group [*pbr-action-group-name*]	Show PBR configuration information
show policy-based-route object [global | interface| [vlan |switchport]|vlan]	Show the PBR configure application information. If the parameter is not specified, it indicates all PBR application information.

46.3 PBR Typical Configuration Example

46.3.1 Configure PBR ***-S -E -A***

Network Requirements

- Device1 has a default route with the gateway of Device2,
- Configure PBR on Device1, so that PC accesses to the network 1.1.1.0/24 via Device3 and accesses to the network 1.1.2.0/24 via Device2.

Network Topology

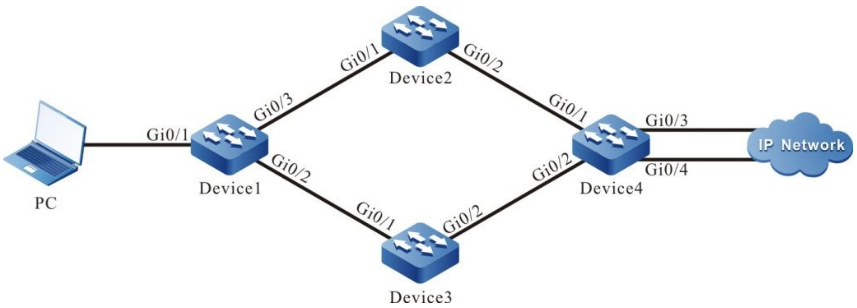


Figure 46-1 Networking for Configuring PBR

Equipment	Port	VLAN	IP address
PC			10.1.1.1/24
Device1	Gi0/1	2	10.1.1.2/24
	Gi0/2	3	20.1.1.1/24
	Gi0/3	4	30.1.1.1/24
Device2	Gi0/1	2	30.1.1.2/24
	Gi0/2	3	50.1.1.1/24
Device3	Gi0/1	2	20.1.1.2/24
	Gi0/2	3	40.1.1.1/24
Device4	Gi0/1	2	50.1.1.2/24
	Gi0/2	3	40.1.1.2/24
	Gi0/3	4	1.1.1.1/24
	Gi0/4	5	1.1.2.1/24

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure static route.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ip route 0.0.0.0 0.0.0.0 30.1.1.2
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ip route 10.1.1.0 255.255.255.0 30.1.1.1
Device2(config)#ip route 1.1.0.0 255.255.0.0 50.1.1.2
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ip route 10.1.1.0 255.255.255.0 20.1.1.1
```

```
Device3(config)#ip route 1.1.0.0 255.255.0.0 40.1.1.2
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#ip route 30.1.1.0 255.255.255.0 50.1.1.1
Device4(config)#ip route 20.1.1.0 255.255.255.0 40.1.1.1
Device4(config)#ip route 10.1.1.0 255.255.255.0 50.1.1.1
Device4(config)#ip route 10.1.1.0 255.255.255.0 40.1.1.1
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is 30.1.1.2 to network 0.0.0.0

S   0.0.0.0/0 [1/100] via 30.1.1.2, 00:26:24, vlan4
C   10.1.1.0/24 is directly connected, 12:00:59 AM, vlan2
C   20.1.1.0/24 is directly connected, 12:00:50 AM, vlan3
C   30.1.1.0/24 is directly connected, 12:00:39 AM, vlan4
C   127.0.0.0/8 is directly connected, 3:47:36 AM, lo0
```

Step 4: Configure PBR on Device1.

#Configure PBR action group and redirect the packet to next hop 20.1.1.2.

```
Device1(config)#pbr-action-group pbr
Device1(config-action-group)#redirect ipv4-nexthop 20.1.1.2
Device1(config-action-group)#count all-colors
Device1(config-action-group)#exit
```

#Query the PBR action group information of Device1.

```
Device1#show pbr-action-group pbr
pbr-action-group pbr
redirect ipv4-nexthop 20.1.1.2(valid)
```

#Configure ACL and bind the ACL rule matching the destination IP network segment 1.1.1.0/24 to L3 action group pbr.

```
Device1(config)#ip access-list extended 1001
Device1(config-std-nacl)#permit ip any 1.1.1.0 0.0.0.255 pbr-action-group pbr
Device1(config-std-nacl)#permit ip any 1.1.2.0 0.0.0.255
Device1(config-std-nacl)#exit
```

#Query the ACL information of Device1.

```
Device1#show ip access-list 1001
```

```
ip access-list standard 1001
 10 permit ip any 1.1.1.0 0.0.0.255 pbr-action-group pbr (active)
 20 permit ip any 1.1.2.0 0.0.0.255
```

Step 6: Apply ACL.

#Apply ACL 1001 on the port vlan2 of Device1.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip policy-based-route 1001 in
Device1(config-if-vlan2)#exit
```

Step 7: Check the result.

#On PC, query the path to destination network 1.1.1.0/24 through Traceroute.

```
C:\Documents and Settings\Administrator>tracert 1.1.1.1

Tracing route to 1.1.1.1 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  10.1.1.2
  2    <1 ms    <1 ms    <1 ms  20.1.1.2
  3    <1 ms    <1 ms    <1 ms  1.1.1.1
Trace complete.
```

As you can see, PC reaches the network 1.1.1.0/24 via Device1, Device3 and Device4.

#On PC, query the path to destination network 1.1.2.0/24 through Traceroute.

```
C:\Documents and Settings\Administrator>tracert 1.1.2.1

Tracing route to 1.1.2.1 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  10.1.1.2
  2    <1 ms    <1 ms    <1 ms  30.1.1.2
  3    <1 ms    <1 ms    <1 ms  1.1.2.1
Trace complete.
```

As you can see, PC reaches the network 1.1.2.0/24 via Device1, Device2 and Device4.

NOTE

- The packets may be flexibly matched according to the quoted ACL rules in terms of packet source IP address, destination IP address, source port, destination port, protocol and TCP flag.

- ACL may be bound to VLAN, Interface VLAN and globally in addition to the two-layer/three-layer Ethernet interface.

47 Route Policy Tools

47.1 Overview

A route policy can change properties or reachability of a route so as to change the routing information or change the paths that the data flow passes. A route policy is mainly applied in the following aspects:

- Sets route properties: Sets the required route properties for the routes that match the route policy.
- Controls route advertisement: When a routing protocol advertises route, it advertises only the routes that meet the requirements.
- Controls route receiving: When a routing protocol, it receives only the routes that meet the requirements so as to control the number of routes and improve the network security.
- Controls route Re-distribution: When a routing protocol Re-distributes external routes, it introduces only the routes that meet the requirements. A route policy tool can also be used to set some properties for the external routes that are introduced.

Key-chain is a password management tool. It provides authentication passwords for the routing protocol to authentication protocol packets.

47.2 Configure Route Policy Tools

Table 47-1 Route Policy Tool List

Configuration task	
Configure Prefix List	Configure Prefix List
Configure AS-PATH list	Configure AS-PATH list
Configure Community-List	Configure Community-List
Configure Extcommunity-List	Configure Extcommunity-List
Configure Route Map	Create Route Map
	Configure the Match Clauses of Route Map
	Configure the Set Clauses of Route Map

Configuration task	
Configure Key Chain	Configure Key Chain

47.2.1 Configure Prefix List *-S -E -A*

Configuration Conditions

None

Configure Prefix List

The prefix list filters routes based on prefixes. The ACL is first designed to filter datagrams and then used to filter routes while the prefix list is designed to filter routes. Through some route filtering functions of the ACL and prefix list are the same, the prefix list is more flexible than the ACL.

A prefix list is identified by a prefix list name. Each prefix list contains multiple entries, and each entry can specify a matching range independently. Each entry has a serial number, indicating the sequence in which the prefix list implements matching checks.

The entries of a prefix list are in the OR relation. When a route tries to match a prefix list, it checks the entries in the sequence of small to large. Once the route matches an entry, it passes the filtration of the prefix list, and the next entry will no longer be checked.

Table 47-2 Configure Prefix List

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure an IPv4 prefix list	**ip prefix-list** *prefix-list-name* [**seq** *seq-value*] { **deny |** **permit** } *network / length* [**ge** *ge-value*] [**le** *le-value*]	Required By default, no IPv4 prefix list is configured

NOTE

- The value range is 0<=length<ge-value<=le-value<=32, where "ge" means equal to or larger than, and "le" means equal to or smaller than. If ip prefix-list test permit 192.168.0.0/16 ge 18 le 24 is configured, it indicates that routes with the address 192.168.0.0 and mask length of 18 to 24 (including 18 and 24) are allowed to pass.
- If network/length is set to 0.0.0.0/0, it means to match the default route. If 0.0.0.0/0 le 32 is configured, it means to match all routes.
- If an implicit expression is contained at the end of an IPv4 prefix list, it means to deny all entries: deny 0.0.0.0/0 le 32. If you want to deny some routes by configuring a deny statement, it is recommended that you add a permit 0.0.0.0/0 le 32 statement to allow

other IPv4 routes to pass.

47.2.2 Configure AS-PATH List *-E -A*

Configuration Conditions

None

Configure AS-PATH List

An AS-PATH list is a tool for filtration based on AS numbers. It is used for BGP route filtration. The AS path property of a BGP route records all ASs that the route passes. When BGP advertises a route to a network outside the local AS, it adds the local AS number to the AS path property to record the AS paths that the route passes.

An AS-PATH list contains multiple entries, and the entries are in the OR relation. When a route tries to match an AS-PATH list, it checks the entries following the sequence of configuration. Once the route matches an entry, it passes the filtration of the AS-PATH list.

Table 47-3 Configure AS-PATH List

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure AS-PATH list	**ip as-path access-list** *path-list-number* { **permit | deny** } *regular-expression*	Required By default, no AS-PATH list is configured.

An AS-PATH list uses a regular expression to specify a collection of AS properties that meet the requirement. A regular expression consists of some common characters and some metacharacters. Common characters http://baike.baidu.com/view/263416.htm include upper- and lower-case characters and numbers while http://baike.baidu.com/view/1061241.htm metacharacters have special meanings, as shown in the following table.

Table 47-4 Meanings of metacharacters in a regular expression

Symbol	Meaning
.	Matches any single character.
*	Matches a sequence which consists of 0 or more bits in the mode.
+	Matches a sequence which consists of 1 or more bits in the mode.

Symbol	Meaning
?	Matches a sequence which consists of 0 or 1 bit in the mode.
^	Matches the start of the inputted character string.
$	Matches the end of the inputted character string.
_	Matches commas, brackets, start and end of the inputted character string, and blank spaces.
[]	Matches single characters in a certain range.
-	Separates the end point of a range.

47.2.3 Configure Community-List *-E -A*

Configuration Conditions

None

Configure Community-List

A Community-list is used to filter community properties of routes. Usually, a route consists of two parts: prefix and routing properties. Routing properties are different for different routing protocols. The IGP protocol usually provides simple properties such as metric, but the BGP protocol provides complex properties such as community property. A Community-list is used for filtration. Filtration on a Community-list acts on the route on which the community property is configured. That is, if the filtration result is deny, the route instead of the community property is filtered.

Two types of Community-lists are available: standard Community-list and extended Community-list. A standard Community-list filters BGP routes based on the local-AS, internet, no-advertise, no-export properties. An extended Community-list filters BGP routes with community properties based on a regular expression.

A Community-list can be used for a routing protocol with community properties. However, you need to bind the Community-list with a route map, and then apply the route map to the routing protocol.

A Community-list contains multiple entries, and the entries are in the OR relation. When a route tries to match a Community-list, it checks the entries following the sequence of configuration. Once the route matches an entry of the community list, it passes the filtration of the community list. For the use of a regular expression in configuring an extended Community-list, refer to "Configure an AS-PATH List".

Table 47-5 Configure Community-List

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure a standard Community-list	**ip community-list** { *community-list-number* | **standard** *community-list-name* } { **permit** | **deny** } [*community-number* / *aa*：*nn* / **local-AS** / **internet** / **no-advertise** / **no-export**]	Required By default, no standard Community-list is configured
Configure an extended Community-list	**ip community-list** { *community-list-number* | **expanded** *community-list-name* } { **permit** | **deny** } *regular-expression*	Required By default, no extended Community-list is configured

47.2.4 Configure Extcommunity-List *-E -A*

Configuration Conditions

None

Configure Extcommunity-List

An extended community list (Extcommunity-list) filters BGP routes based on the extended community properties. The quality and usage method of an extended community list (Extcommunity-list) are the same as a standard community list. The major difference is that extended community properties are mainly used in an MPLS L3VPN, so an Extcommunity list is also mainly used in an MPLS L3VPN.

Two types of Extcommunity-lists are available: standard Extcommunity-list and extended Extcommunity-list. The standard Extcommunity-list filters BGP routes based on Router Target and Site of Origin properties. An extended Extcommunity-list filters BGP routes with community properties based on a regular expression.

An Extcommunity-list contains multiple entries, and the entries are in the OR relation. When a route tries to match an Extcommunity-list, it checks the entries following the sequence of configuration. Once the route matches an entry, it passes the filtration of the Extcommunity-list. For the use of a regular expression in configuring an extended Extcommunity-list, refer to "Configure an AS-PATH List".

Table 47-6 Configure Extcommunity-List

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Configure a standard Extcommunity-list.	**ip extcommunity-list** { *extcommunity-list-number* | **standard** *extcommunity-list-name*} { **permit | deny** } [**rt** *extcommunity-number* / **soo** *extcommunity-number*]	Required By default, no standard Extcommunity-list is configured.
Configure an extended Extcommunity list.	**ip extcommunity-list** { *extcommunity-list-number* **| expanded** *extcommunity-list-name* } { **permit | deny** } *regular-expression*	Required By default, no extended Extcommunity-list is configured.

47.2.5 Configure Route Map *-S -E -A*

A route map is a tool for matching routes and setting route properties. A route map consists of multiple statements, and each statement consists of some match clauses and set clauses. The match clauses define the matching rules of the statement, and the set clauses define the follow-up actions after a route match the match clauses. The match clauses are in the OR relation, that is, a route must match all match clauses of the statement.

The route map statements are in the OR relation. When a route tries to match a route map, it checks the entries in the sequence of small to large. Once a route matches a statement, it matches the route map, and the next statement will no longer be checked. If a route fails to match a statement, it fails to match the route map.

Configuration Conditions

Before configuring a route map, ensure that:

- The ACL, prefix list, AS-PATH, and Community-list or Extcommunity-list that are required for configuring a route map have been configured.

Create Route Map

In creating a route map, you can specify the match mode of the statements of the route map. Two match modes are available: permit and deny.

The **permit** mode sets the matching mode of the statements of the route map to permit, that is, if a route matches all match clauses of the statement, the route is allowed to pass, and then the set clauses of the statement are executed. If a route fails to match the match clauses of the statement, it starts to match the next statement of the route map;

The **deny** mode sets the matching mode of the statements of the route map to deny, that is, when a route matches all match clauses of a statement, the route is denied, and the route will not match the next statement of the route map. In **deny** mode, set clauses will not be executed.

Table 47-7 Create Route Map

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create Route Map	**route-map** *map-name* [{ **permit** | **deny** } [*seq-number*]]	Required By default, no route map is created.

NOTE

- If you run the route-map command to create a route map, if you configure only the route map name but do not configure the match mode and statement serial number, a statement whose match mode is permit and serial number is 10 is automatically created.
- If a route map is applied to the routing protocol but the route map has not been configured, all objects will fail to match.

Configure the Match Clauses of Route Map

The match clauses of a route map statement are in the OR relation, that is, a route must match all match clauses before it is allowed to pass.

Table 47-8 Configure the Match Clause of Route Map

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the route map configuration mode	**route-map** *map-name* [{ **permit** | **deny** } [*seq-number*]]	-
Specify the AS-PATH list that the route map matches.	**match as-path** *path-list-number*	Optional By default, no AS-PATH list that the route map matches is specified.
Specify the BGP Community-list that the route map matches.	**match community** *community-list-number* / *community-list-name* [**exact-match**]	Optional By default, no BGP Community-list that the route map matches is specified.

Steps	Command	Description
Specify the BGP Extcommunity-list that the route map matches.	**match extcommunity** ext*community-list-number* / ext*community-list-name*	Optional By default, no BGP Extcommunity-list that the route map matches is specified.
Specify the interface that the route map matches.	**match interface** *interface-names*	Optional By default, no interface that the route map matches is specified.
Specify the route prefix that the route map matches.	**match ip address** { *access-list-number* | *access-list-name* | **prefix-list** *prefix-list-name* }	Optional By default, no route prefix that the route map matches is specified.
Specify the next-hop address that the route map matches.	**match ip next-hop** { *access-list-name* | **prefix-list** *prefix-list-name* }	Optional By default, no next-hop address that the route map matches is specified.
Specify the source route address that the route map matches.	**match ip route-source** { *access-list-name* | **prefix-list** *prefix-list-name* }	Optional By default, no source route address that the route map matches is specified.
Specify the route metric value that the route map matches.	**match metric** *metric-value* [**+-***offset*]	Optional By default, no route metric value that the route map matches is specified.
Specify the routing type that the route map matches.	**match route-type** { **external** / **interarea** / **internal** / **level-1** / **level-2** / **nssa-external** / **type-1** / **type-2** }	Optional By default, no routing type that the route map matches is specified.
Specify the tag value that the route map matches.	**match tag** *tag-value*	Optional By default, no tag value that the route map matches is specified.

NOTE

- If a route map is not configured with match clauses, all objects can match the route map successfully.
- When the ACL and prefix list that are associated with the match clauses do not exist, no object can match the route map.

Configure the Set Clauses of Route Map

When the route map match mode is permit, if a route matches all match clauses, the set operations will be executed. If the match mode is deny, the set operations will not be performed.

Table 47-9 Configure the Set Clauses of Route Map

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the route map configuration mode	**route-map** *map-name* [{ **permit** | **deny** } [*seq-number*]]	-
Set the AS path property of a BGP route.	**set as-path prepend** *as-path-number*	Optional By default, the AS path property of the BGP route is not configured.
Configure the community property of the BGP route.	**set communtiy** { *community-number* | **additive** | **local-AS** | **internet** | **no-advertise** | **no-export** | **none** }	Optional By default, the community property of the BGP route is not configured.
Delete the Community-list of the BGP route.	**set comm-list** { *community-list-number* / *community-list-name* } **delete**	Optional By default, the community property of the BGP route is not deleted.
Set BGP route attenuation parameters.	**set dampening** *half-life start-reusing start-suppress max-duration*	Optional By default, BGP route attenuation parameters are not set.

Steps	Command	Description
Set Extcommunity properties of the MPLS L3VPN route.	**set extcommunity** { **rt** | **soo** } *extcommunity*	Optional By default, the Extcommunity properties of MPLS L3VPN are not configured.
Set the next hop for the route.	**set ip default next-hop** *ip-address*	Optional By default, the next hop for the route is not configured. It is used to set the next hop during the OSPF route redistributing
Set the next hop for the route.	**set ip next-hop** *ip-address*	Optional By default, the next hop for the route is not configured. It is used to set the route next hop for the BGP associated route map.
Set the local priority of BGP route.	**set local-preference** *value*	Optional By default, the local priority is not configured for the BGP route.
Set the metric value of the route.	**set metric** { *metric* | *+metric* | *-metric* | *bandwidth delay reliable loading mtu* }	Optional By default, the metric value of the route is not configured.
Set the metric type of the route.	**set metric-type** { **external** | **internal** | **type-1** | **type-2** }	Optional By default, the metric type of the route is not configured.
Set the Origin property of the BGP route.	**set origin** { **egp** *as-number* | **igp** | **incomplete** }	Optional By default, the Origin property of the BGP route is not set.

Steps	Command	Description
Set the tag option field of external routes.	**set tag** *tag-value*	Optional By default, the tag option field of external routes is not configured.
Set the weight of the BGP route.	**set weight** *weight-value*	Optional By default, the weight of the BGP route is not configured.

47.2.6 Configure Key Chain *-S -E -A*

Configuration Conditions

None

Configure Key Chain

Key chain is a password management tool. It provides authentication passwords for the routing protocol to authentication protocol packets. A key chain provides different passwords for transmitting and receiving packets, and it provides different passwords for different Key IDs. Meanwhile, a key chain can automatically switch passwords according to the validity duration of keys, that is, it uses different keys in different periods of time. This greatly enhances the password security.

You can configure multiple Key IDs for a key chain. When a protocol uses the key chain for authentication, it obtains the Key ID according to the following rules:

- The minimum valid transmit passwords of the Key IDs are obtained as the transmit passwords.
- Among the Key IDs that are larger than the specified key IDs of the protocol, obtain the minimum valid receive passwords of the Key IDs as the receive passwords.
- If a Key ID is contained in the received protocol packets, a search for the valid receive passwords are performed based on the Key ID. Otherwise, the minimum valid receive passwords of the Key IDs in the local key chain is used as the receive password.

Table 47-10 Configure Key Chain

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure a key chain.	**key chain** *keychain-name*	Required By default, the key chain is not configured.

Steps	Command	Description
Configure a Key ID.	**key** *key-id*	Required By default, the Key ID is not configured.
Configure a password	**key-string** [**0 | 7**] *password*	Required By default, no password is configured. A blank space is also regarded as a password character. Pay attention to this while configuring a password.
Configure the valid duration in which a key acts as the receive password.	**accept-lifetime** *time-start* { *time-end* **| duration** *second* **| infinite** }	Required By default, the receive password is always valid.
Configure the valid duration in which a key acts as the transmit password.	**send-lifetime** *time-start* { *time-end* **| duration** *second* **| infinite** }	Required By default, the transmit password is always valid.

47.2.7 Route Policy Monitoring and Maintaining -S -E -A

Table 47-11 Route Policy Monitoring and Maintaining

Command	Description
clear ip prefix-list [*prefix-list-name network/length*]	Clear the prefix list statistics
show ip prefix-list [*prefix-list-name* [*network/lenghter* [**first-match | longer**] **| seq** *sep_value*] **| detail** [*prefix-list-name*] **| orf-prefix | summary** [*prefix-list-name*]	Display the information about a prefix list
show ip as-path-access-list [*list-name*]	Display the information about an AS-PATH list
show ip community-list [*community-list-number* | *community-list-name*]	Display the information about a Community list

Command	Description
show ip extcommunity-list [*extcommunity-list-number* | *extcommunity-list-name*]	Display the information about an Extcommunity list
show route-map [*route-map-name*]	Display the information about a route map
show key chain [*keychain-name*]	Display the information about a key chain

47.3 Route Policy Tool Typical Configuration Example

47.3.1 Configure Route Redistribution with Route Policy *-S -E -A*

Network Requirements

- Run OSPF between Device1 and Device2, and run RIP between Device2 and Device3.
- On Device2, configure OSPF to Re-distribute RIP routes, and associate a route policy to modify route properties. It is required that the tag property of route 100.1.1.0/24 is changed to 5, the metric value of route 110.1.1.0/24 is changed to 50, and the property of route 120.1.1.0/24 keeps unchanged.

Network Topology

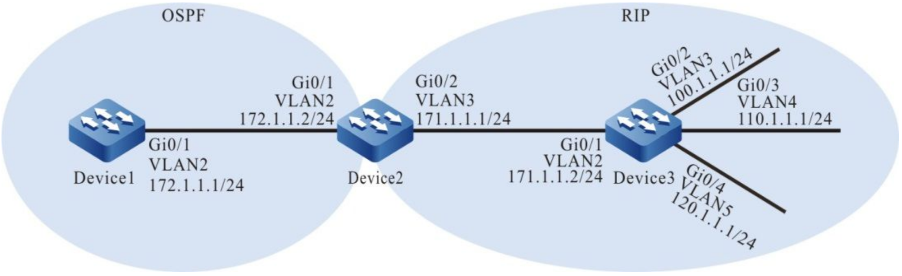


Figure 47-1 Configuring Route Redistribution with Route Policy

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
```

```
Device1(config-ospf)#network 172.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 172.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

Step 4: Configure RIP.

#Configure Device2.

```
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 171.1.1.0
Device2(config-rip)#exit
```

#Configure Device3.

```
Device3(config)#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 171.1.1.0
Device3(config-rip)#network 100.1.1.0
Device3(config-rip)#network 110.1.1.0
Device3(config-rip)#network 120.1.1.0
Device3(config-rip)#exit
```

Step 5: Configure OSPF to re-distribute RIP routes.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip
Device2(config-ospf)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

OE  100.1.1.0/24 [150/20] via 172.1.1.2, 2:22:08 AM, vlan2
OE  110.1.1.0/24 [150/20] via 172.1.1.2, 12:49:57 AM, vlan2

OE  120.1.1.0/24 [150/20] via 172.1.1.2, 2:22:08 AM, vlan2

OE  171.1.1.0/24 [150/20] via 172.1.1.2, 2:22:41 AM, vlan2
```

According to the routing table of Device1, the RIP routes 100.1.1.0/24, 110.1.1.0/24, and 120.1.1.0/24 on Device2 are Re-distributed to the OSPF process and successfully advertised to Device1.

Step 6: Configure an ACL and route policy.

#Configure Device2.

Configure an ACL to allow routes 100.1.1.0/24, 110.1.1.0/24, and 120.1.1.0/24 to pass.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.1.1.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#ip access-list standard 2
Device2(config-std-nacl)#permit 110.1.1.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#ip access-list standard 3
Device2(config-std-nacl)#permit 120.1.1.0 0.0.0.255
Device2(config-std-nacl)#exit
```

Configure route policy rip_to_ospf. Set the tag property of the routes that match ACL 1, set the metric property of the routes that match ACL2, and do not change the routing properties of the routes that match ACL 3.

```
Device2(config)#route-map rip_to_ospf 10
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#set tag 5
Device2(config-route-map)#exit
Device2(config)#route-map rip_to_ospf 20
Device2(config-route-map)#match ip address 2
Device2(config-route-map)#set metric 50
Device2(config-route-map)#exit
Device2(config)#route-map rip_to_ospf 30
Device2(config-route-map)#match ip address 3
Device2(config-route-map)#exit
```

NOTE

- In configuring a route policy, you can create a matching rule based on a prefix list or ACL. The prefix list can precisely match routing masks while the ACL cannot match routing masks.

Step 7: Configure OSPF to re-distribute RIP routes and associate a route policy.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip route-map rip_to_ospf
Device2(config-ospf)#exit
```

Step 8: Check the result.

#Check the OSPF database of Device1.

```
Device1#show ip ospf database external
      OSPF Router with ID (172.1.1.1) (Process ID 100)


        AS External Link States



  LS age: 1183
 Options: 0x22 (-|-|DC|-|-|-|E|-)
 LS Type: AS-external-LSA
 Link State ID: 100.1.1.0 (External Network Number)
 Advertising Router: 172.1.1.2
 LS Seq Number: 80000006
 Checksum: 0xbcc0
 Length: 36
 Network Mask: /24
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 20
    Forward Address: 0.0.0.0
    External Route Tag: 5



 LS age: 1233
 Options: 0x22 (-|-|DC|-|-|-|E|-)
 LS Type: AS-external-LSA
 Link State ID: 110.1.1.0 (External Network Number)
 Advertising Router: 172.1.1.2
 LS Seq Number: 80000006
 Checksum: 0x0d4d
 Length: 36
```

```
Network Mask: /24
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 50
      Forward Address: 0.0.0.0
      External Route Tag: 0



LS age: 1113
Options: 0x22 (-|-|DC|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 120.1.1.0 (External Network Number)
Advertising Router: 172.1.1.2
LS Seq Number: 80000005
Checksum: 0x5f10
Length: 36
Network Mask: /24
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 20
      Forward Address: 0.0.0.0
      External Route Tag: 0
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

OE  100.1.1.0/24 [150/20] via 172.1.1.2, 2:30:28 AM, vlan2
OE  110.1.1.0/24 [150/50] via 172.1.1.2, 12:58:17 AM, vlan2
OE  120.1.1.0/24 [150/20] via 172.1.1.2, 2:30:28 AM, vlan2
```

According to the OSPF database and routing table of Device1, the tag of route 100.1.1.0/24 is 5, the metric of route 110.1.1.0/24 is 50, and the routing properties of route 120.1.1.0/24 are not changed.

NOTE

- In redistributing external routes, the routes of the direct connect interfaces that are covered by the RIP process will also be Re-distributed into the target protocol.

47.3.2 Configure Route Policy for BGP -E -A

Network Requirements

- Run IGP protocol OSPF and set up IBGP neighbors between Device1 and Device2 and between Device1 and Device3, and set up EBGP neighbors between Device4 and Device2 and between Device4 and Device3.
- Configure a route policy on Device2 and Device3 so that the data of Device1 reaches network segment 100.1.1.0/24 through Device2, reaches network segment 110.1.1.0/24 through Device3, and the data of Device4 reaches network segment 120.1.1.0/24 through Device2, and reaches network segment 130.1.1.0/24 through Device3.

Network Topology

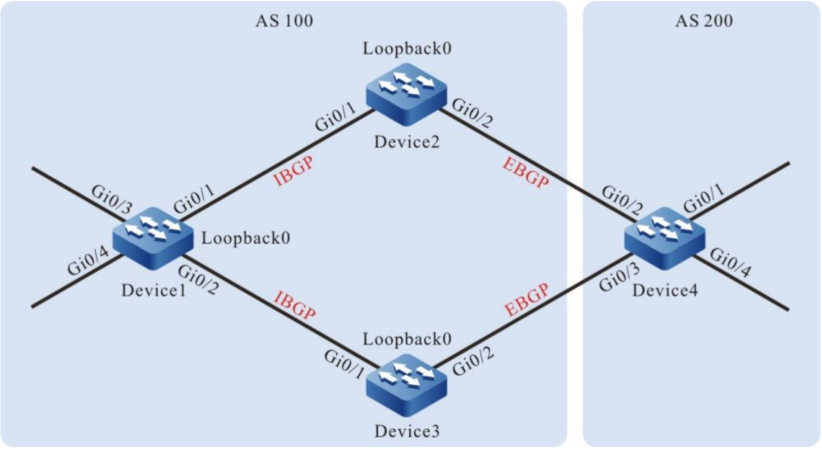


Figure 47-2 Configuring a Route Policy for BGP

Equipment	Interface	VLAN	IP address
Device1	Gi0/1	2	1.0.0.1/24
	Gi0/2	3	2.0.0.1/24
	Gi0/3	4	120.1.1.1/24
	Gi0/4	5	130.1.1.1/24
	Loopback0		38.1.1.1/32
Device2	Gi0/1	2	1.0.0.2/24
	Gi0/2	3	3.0.0.1/24
	Loopback0		39.1.1.1/32

Equipment	Interface	VLAN	IP address
Device3	Gi0/1	2	2.0.0.2/24
	Gi0/2	3	4.0.0.1/24
	Loopback0		40.1.1.1/32
Device4	Gi0/1	2	100.1.1.1/24
	Gi0/2	3	3.0.0.2/24
	Gi0/3	4	4.0.0.2/24
	Gi0/4	5	110.1.1.1/24

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure OSPF to make the Loopback routes between the devices are mutually reachable.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 38.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 39.1.1.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
```

```
Device3(config-ospf)#network 40.1.1.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set


O   39.1.1.1/32 [110/2] via 1.0.0.2, 7:11:33 PM, vlan2
O   40.1.1.1/32 [110/2] via 2.0.0.2, 6:56:32 PM, vlan3
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
O   2.0.0.0/24 [110/2] via 1.0.0.1, 7:19:10 PM, vlan2
O   38.1.1.1/32 [110/2] via 1.0.0.1, 7:09:43 PM, vlan2
O   40.1.1.1/32 [110/3] via 1.0.0.1, 6:56:49 PM, vlan2
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
O   1.0.0.0/24 [110/2] via 2.0.0.1, 7:17:33 PM, vlan2
O   38.1.1.1/32 [110/2] via 2.0.0.1, 7:09:59 PM, vlan2
O   39.1.1.1/32 [110/3] via 2.0.0.1, 7:12:06 PM, vlan2
```

After the configuration is completed, Device1 can set up OSPF neighbors respectively with Device2 and Device3 and the devices can learn the Loopback routes of the peer end.

Step 4: Configure BGP.

#Configure Device1.

Configure Device1 to set up IBGP neighbors respectively with Device2 and Device3 through Loopback interfaces and advertise routes 120.1.1.0/24 and 130.1.1.0/24 to the BGP routing table.

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 39.1.1.1 remote-as 100
Device1(config-bgp)#neighbor 39.1.1.1 update-source loopback0
Device1(config-bgp)#neighbor 40.1.1.1 remote-as 100
```

```
Device1(config-bgp)#neighbor 40.1.1.1 update-source loopback0

Device1(config-bgp)#network 120.1.1.0 255.255.255.0

Device1(config-bgp)#network 130.1.1.0 255.255.255.0

Device1(config-bgp)#exit
```

#Configure Device2.

```
Device2(config)#router bgp 100

Device2(config-bgp)#neighbor 38.1.1.1 remote-as 100

Device2(config-bgp)#neighbor 38.1.1.1 update-source loopback0

Device2(config-bgp)#neighbor 38.1.1.1 next-hop-self

Device2(config-bgp)#neighbor 3.0.0.2 remote-as 200

Device2(config-bgp)#exit
```

#Configure Device3.

```
Device3(config)#router bgp 100

Device3(config-bgp)#neighbor 38.1.1.1 remote-as 100

Device3(config-bgp)#neighbor 38.1.1.1 update-source loopback0

Device3(config-bgp)#neighbor 38.1.1.1 next-hop-self

Device3(config-bgp)#neighbor 4.0.0.2 remote-as 200

Device3(config-bgp)#exit
```

#Configure Device4.

Configure Device4 to set up EBGP neighbors respectively with Device2 and Device3 and advertise routes 100.1.1.0/24 and 110.1.1.0/24 to the BGP routing table.

```
Device4#configure terminal

Device4(config)#router bgp 200

Device4(config-bgp)#neighbor 3.0.0.1 remote-as 100

Device4(config-bgp)#neighbor 4.0.0.1 remote-as 100

Device4(config-bgp)#network 100.1.1.0 255.255.255.0

Device4(config-bgp)#network 110.1.1.0 255.255.255.0

Device4(config-bgp)#exit
```

#Query the BGP route information of Device1.

```
Device1#show ip bgp

BGP table version is 2, local router ID is 38.1.1.1

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

        S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path

[B]*>i100.1.1.0/24       39.1.1.1              0    100      0 200 i

[B]* i                  40.1.1.1              0    100      0 200 i

[B]*>i110.1.1.0/24       39.1.1.1              0    100      0 200 i

[B]* i                  40.1.1.1              0    100      0 200 i

[B]*> 120.1.1.0/24       0.0.0.0               0         32768 i
```

```
[B]*> 130.1.1.0/24       0.0.0.0              0        32768 i
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   100.1.1.0/24 [200/0] via 39.1.1.1, 7:03:19 PM, vlan2
B   110.1.1.0/24 [200/0] via 39.1.1.1, 7:03:19 PM, vlan2
```

According to the BGP routing table of Device1, data that are targeted at network segments 100.1.1.0/24 and 110.1.1.0/24 have two valid routes respectively. Because the router ID of Device2 is smaller, the BGP data that are targeted at network segments 100.1.1.0/24 and 110.1.1.0/24 choose to pass Device2 by default.

#Query the BGP route information of Device4.

```
Device4#show ip bgp
BGP table version is 3, local router ID is 110.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network           Next Hop          Metric LocPrf Weight Path
[B]*> 100.1.1.0/24       0.0.0.0              0        32768 i
[B]*> 110.1.1.0/24       0.0.0.0              0        32768 i
[B]*  120.1.1.0/24       4.0.0.1              0            0 100 i
[B]*>                 3.0.0.1              0           0 100 i
[B]*  130.1.1.0/24       4.0.0.1              0            0 100 i
[B]*>                 3.0.0.1              0           0 100 i
```

#Query the routing table of Device4.

```
Device4#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   120.1.1.0/24 [20/0] via 3.0.0.1, 7:25:05 PM, vlan3
B   130.1.1.0/24 [20/0] via 3.0.0.1, 7:25:05 PM, vlan3
```

According to the BGP routing table of Device4, the data that are targeted at network segments 120.1.1.0/24 and 130.1.1.0/24 have two valid routes. Because Device4 first sets up a neighbor relation with Device2 and it takes longer time for Device2 to learn the two routes, BGP data that are targeted at the network segments 120.1.1.0/24 and 130.1.1.0/24 choose to pass Device2 by default.

Step 5: Configure a prefix list and route policy.

#Configure Device2.

Configure a prefix list to allow routes 100.1.1.0/24 and 130.1.1.0/24 to pass.

```
Device2(config)#ip prefix-list 1 permit 100.1.1.0/24
Device2(config)#ip prefix-list 2 permit 130.1.1.0/24
```

Configure the route policy lp so that the prefix list 1 of Device2 allows setting local-preference for routes.

```
Device2(config)#route-map lp 10
Device2(config-route-map)#match ip address prefix-list 1
Device2(config-route-map)#set local-preference 200
Device2(config-route-map)#exit
Device2(config)#route-map lp 20
Device2(config-route-map)#exit
```

Configure the route policy med so that the prefix list 2 of Device2 allows setting the MED property for routes.

```
Device2(config)#route-map med 10
Device2(config-route-map)#match ip address prefix-list 2
Device2(config-route-map)#set metric 10
Device2(config-route-map)#exit
Device2(config)#route-map med 20
Device2(config-route-map)#exit
```

#Configure Device3.

Configure a prefix list to allow routes 110.1.1.0/24 and 120.1.1.0/24 to pass.

```
Device3(config)#ip prefix-list 1 permit 110.1.1.0/24
Device3(config)#ip prefix-list 2 permit 120.1.1.0/24
```

Configure the route policy lp so that the prefix list 1 of Device3 allows setting local-preference for routes.

```
Device3(config)#route-map lp 10
Device3(config-route-map)#match ip address prefix-list 1
Device3(config-route-map)#set local-preference 200
Device3(config-route-map)#exit
Device3(config)#route-map lp 20
Device3(config-route-map)#exit
```

Configure the route policy med so that the prefix list 2 of Device3 allows setting the MED property for routes.

```
Device3(config)#route-map med 10
Device3(config-route-map)# match ip address prefix-list 2
Device3(config-route-map)#set metric 10
Device3(config-route-map)#exit
Device3(config)#route-map med 20
```

```
Device3(config-route-map)#exit
```

NOTE

- In configuring a route policy, you can create a matching rule based on a prefix list or ACL. The prefix list can precisely match routing masks while the ACL cannot match routing masks.

Step 6: Configure route policy for BGP.

#Configure Device2.

Apply the route policy lp to the outgoing routes of neighbor 38.1.1.1 and apply the route policy med to the outgoing routes of neighbor 3.0.0.2.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 38.1.1.1 route-map lp out
Device2(config-bgp)#neighbor 3.0.0.2 route-map med out
Device2(config-bgp)#exit
```

#Configure Device3.

Apply the route policy lp to the outgoing routes of neighbor 38.1.1.1 and apply the route policy med to the outgoing routes of neighbor 4.0.0.2.

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 38.1.1.1 route-map lp out
Device3(config-bgp)#neighbor 4.0.0.2 route-map med out
Device3(config-bgp)#exit
```

Step 7: Check the result.

#Query the BGP route information of Device1.

```
Device1#show ip bgp
BGP table version is 9, local router ID is 38.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
          S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
[B]* i100.1.1.0/24       40.1.1.1              0    100      0 200 i
[B]*>i                 39.1.1.1              0    200      0 200 i
[B]*>i110.1.1.0/24       40.1.1.1              0    200      0 200 i
[B]* i                 39.1.1.1              0    100      0 200 i
[B]*> 120.1.1.0/24       0.0.0.0               0       32768 i
```

```
[B]*> 130.1.1.0/24       0.0.0.0                0        32768 i
```

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   100.1.1.0/24 [200/0] via 39.1.1.1, 2:58:12 AM, vlan2
B   110.1.1.0/24 [200/0] via 40.1.1.1, 2:58:10 AM, vlan3
```

According to the BGP routing table of Device1, route 100.1.1.0/24 has two next hops, 40.1.1.1 and 39.1.1.1. The local-preference of the route with the next hop 39.1.1.1 has been changed to 200 so that the data that are targeted at the network segment 100.1.1.0/24 choose to pass Device2 with priority. Route 110.1.1.0/24 also has two next hops, 40.1.1.1 and 39.1.1.1. The local-preference of the route with the next hop 40.1.1.1 has been changed to 200 so that the data that are targeted at the network segment 110.1.1.0/24 choose to pass Device3 with priority.

#Query the BGP route information of Device4.

```
Device4#show ip bgp
BGP table version is 9, local router ID is 110.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network            Next Hop          Metric LocPrf Weight Path
[B]*> 100.1.1.0/24       0.0.0.0                0        32768 i
[B]*> 110.1.1.0/24       0.0.0.0                0        32768 i
[B]*  120.1.1.0/24       4.0.0.1               10            0 100 i
[B]*>                    3.0.0.1                0            0 100 i
[B]*> 130.1.1.0/24       4.0.0.1                0            0 100 i
[B]*                     3.0.0.1               10            0 100 i
```

#Query the routing table of Device4.

```
Device4#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   120.1.1.0/24 [20/0] via 3.0.0.1, 3:05:39 AM, vlan3
B   130.1.1.0/24 [20/0] via 4.0.0.1, 3:05:37 AM, vlan4
```

According to the BGP routing table of Device4, route 120.1.1.0/24 has two next hops, 4.0.0.1 and 3.0.0.1. The metric of the route with the next hop 4.0.0.1 has been changed to 10 so that the data that are targeted at the network segment 120.1.1.0/24 choose to pass Device2 with priority. Route

130.1.1.0/24 also has two next hops, 4.0.0.1 and 3.0.0.1. The metric of the route with the next hop 3.0.0.1 has been changed to 10 so that the data that are targeted at the network segment 130.1.1.0/24 choose to pass Device3 with priority.

NOTE

- If a route policy is applied to a BGP peer or peer group, it can be applied in the receiving or advertisement direction of the BGP peer or peer group, and the settings take effect after BGP is reset.

48 L2 Multicast Basics

48.1 Overview

The main task of L2 multicast basis is to maintain the L2 multicast forwarding table. The application modules of L2 multicast generates their L2 multicast tables by static configuration and dynamic learning, and then synchronize the information to the L2 multicast basis modules. L2 multicast basis modules integrate the information to form the L2 multicast forwarding table.

48.2 L2 Multicast Basics Function Configuration

Table 481 Configuration list of L2 multicast basics

Configuration Task	
Configure the unknown packet forwarding policy of L2 multicast	Configure unknown packet MAC forwarding policy of L2 multicast
	Configure unknown packet IP forwarding policy of L2 multicast
Configure L2 static multicast	Configure L2 static multicast

48.2.1 Configure Unknown Packet Forwarding Policy of L2 Multicast

-B -S -E -A

Unknown multicast service packets have two kinds of forwarding policies: drop unknown multicast service packets, or make the unknown multicast service packets flood.

Configuration Conditions

Before configuring the unknown packet forwarding policy of L2 multicast, first complete the following task:

- Configure corresponding VLAN

Configure Unknown Packet MAC Forwarding Policy of L2 Multicast

In the L2 multicast MAC forwarding mode, the multicast service packets are forwarded by matching VLAN and destination MAC address. When the multicast service packet does not match the forwarding table, it is unknown multicast service packet. The device has two kinds of forwarding policies for the unknown multicast service packets: drop unknown multicast service packets, or make unknown multicast service packets flood.

Table 482 Configure unknown packet MAC forwarding policy of L2 multicast

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter VLAN configuration mode	**vlan** *vlan-id*	-
Configure L2 multicast forwarding policy	**l2-multicast drop-unknown**	Optional By default, the function of dropping unknown multicast service packets is not enabled in VLAN.

Configure Unknown Packet IP Forwarding Policy of L2 Multicast

In the L2 multicast IP forwarding mode, the multicast service packets are forwarded by matching VLAN, multicast source IP address and multicast destination IP address. When the multicast service packet does not match the forwarding table, it is unknown multicast service packet. The device has two kinds of forwarding policies for the unknown multicast service packets: drop unknown multicast service packets, or make unknown multicast service packets flood.

Table 483 Configure unknown packet IP forwarding policy of L2 multicast

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter VLAN configuration mode	**vlan** *vlan-id*	-
Configure L2 multicast IP forwarding policy	**l3-multicast drop-unknown**	Mandatory By default, the function of dropping unknown multicast service packets is not enabled in VLAN.

48.2.2 Configure L2 Static Multicast *-B -S -E -A*

L2 static multicast generates L2 multicast forwarding table by static configuration. It is formed by the user specifying multicast MAC address, VLAN, and port list (including member port list and prohibited port list).

Configuration Conditions

Before configuring L2 static multicast, first complete the following task:

- Configure corresponding VLAN

Configure L2 static multicast

Table 484 Configure L2 static multicast

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Create L2 static multicast	**l2-multicast mac-entry static** *mac-address* **vlan** *vlan-id*	Mandatory By default, L2 static multicast entry is not configured.
Configure member port of L2 static multicast entry	**interface** *interface-list-name* { **member | forbidden** }	Optional By default, the member port of L2 static multicast entry is not configured.
Configure member aggregation group of L2 static multicast entry	**link-aggregation** *link-aggregation-id* { **member | forbidden** }	Optional By default, the member aggregation group of L2 static multicast entry is not configured.

48.2.3 Monitoring and Maintaining of L2 Multicast Basis *-B -S -E -A*

Table 485 Monitoring and maintaining of L2 multicast basis

Command	Description
show l2-multicast ip-entry	Display the IP forwarding table information of L2 multicast

Command	Description
show l2-multicast l3-ip-entry	Display the L3 IP forwarding table information of L2 multicast
show l2-multicast mac-entry { **all** | **forward** | **static** }	Display the L2 multicast table

48.3 Typical Configuration Example of L2 Static Multicast

48.3.1 Configure L2 Static Multicast *-B -S -E -A*

Network Requirements

- Device1 configures multicast routing protocol; Device2 configures L2 static multicast in VLAN2; PC1 is the receiver of multicast service; PC2 and PC3 are not the receiver of multicast service.
- Multicast Server sends multicast service packets; PC1 can receive multicast service packets correctly; PC2 and PC3 cannot receive multicast service packets.

Network Topology

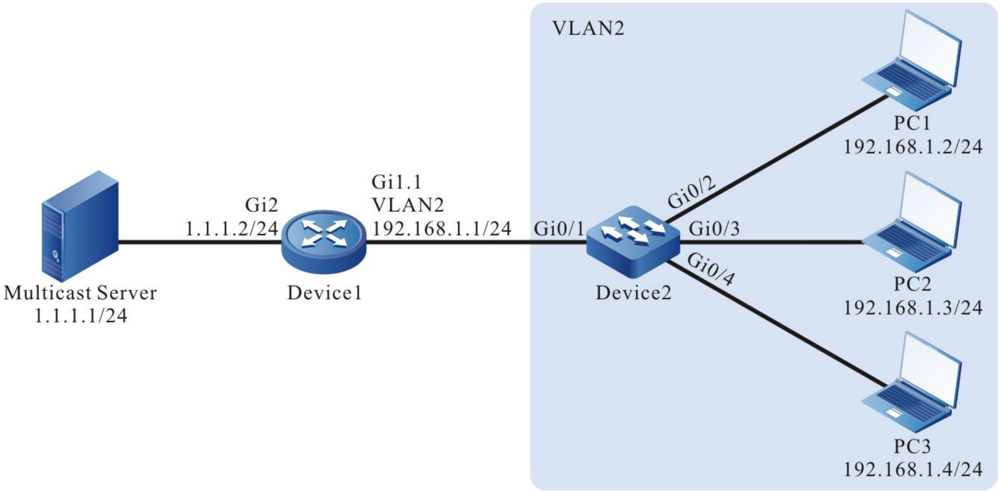


Figure 481 Network topology of configuring L2 static multicast

Configuration Steps

Step 1: Device1 configures interface IP address and enables multicast routing protocol. (omitted)

Step 2: Configure Device2.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/2 - gigabitethernet0/4 on Device2 as Access, permitting the services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Trunk, permitting the services of VLAN2 to pass. Configure PVID as 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable dropping unknown multicast in VLAN2.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Configure the members of L2 static multicast group.

```
Device2(config)#l2-multicast mac-entry static 0100.5E01.0101 vlan 2
Device2(config-mcast)#interface gigabitethernet 0/2 member
Device2(config-mcast)#exit
Device2(config)#l2-multicast mac-entry static 0100.5E01.0101 vlan 2
Device2(config-mcast)#interface gigabitethernet 0/3 forbidden
Device2(config-mcast)#exit
```

Step 3: Check the result.

#View the L2 static multicast entry of Device2.

```
Device2#show l2-multicast mac-entry static
Current L2 Static Multicast 2 entries

---- -------- ------------------ ------------------------------
NO.  VID      Group MAC address  Interface Name
---- -------- ------------------ ------------------------------
1    2        0100.5E01.0101     [M] gigabitethernet0/2
2    2        0100.5E01.0101     [F] gigabitethernet0/3
```

#Multicast Server sends the multicast service packets with destination address 224.1.1.1. PC1 can receive the multicast service packets correctly; PC2 and PC3 cannot receive multicast service packets.

49 IGMP snooping

49.1 Overview

IGMP Snooping (Internet Group Management Protocol snooping) is the function designed for the device that does not support IGMP to reduce the spreading range of the multicast service packet and prevent the multicast packet from being spread to the network segments that do not need the multicast packet. It forms and maintains the downstream member port list of each multicast group at the local by listening to IGMP packets. In this way, when receiving multicast service packet, forward at the specified downstream member port. Meanwhile, IGMP Snooping can listen to the IGMP protocol packets and cooperate with the upstream multicast router to manage and control multicast services.

IGMP Snooping mainly realizes the following functions:

- Listen to the IGMP packets to set up multicast information. IGMP Snooping gets the downstream multicast receiver information by listening to IGMP packets, realizing the forwarding of multicast service packets at the specified member port.
- Listen to the IGMP protocol packets. In this way, the upstream multicast router can correctly maintain IGMP member relation table.

49.2 IGMP snooping Function Configuration

Table 491 IGMP snooping function configuration list

Configuration Task	
Configure basic functions of IGMP Snooping	Enable the IGMP Snooping function
	Configure the IGMP snooping version
	Enable the IGMP snooping IP forwarding function
Configure IGMP snooping querier	Enable the IGMP snooping querier
	Configure the source IP address of the IGMP query packet
	Configure general group query interval
	Configure the maximum response time

Configuration Task	
	Configure the query interval of the specified group
	Configure fast-leave
Configure IGMP snooping router port	Configure IGMP snooping router port
	Configure the age time of IGMP snooping dynamic router port
Configure IGMP snooping TCN event	Enable fast convergence
	Configure the query interval of TCN event
	Configure the query times of TCN event
Configure IGMP snooping policy	Configure the port filter rule
	Configure maximum items of port multicast group
	Configure the upper-limiting policy of port multicast group
Configure IGMP snooping proxy	Configure the IGMP snooping proxy

49.2.1 Configure IGMP snooping Basic Functions *-B -S -E -A*

In the configuration tasks of IGMP snooping, you should first enable the IGMP snooping function so that the configuration of the other functions can take effect.

Configuration Conditions

Before configuring the basic functions of IGMP snooping, first complete the following task:

- Configure VLAN

Enable IGMP snooping Function

After enabling IGMP snooping function, the device can run the IGMP snooping function.

Table 492 Enable IGMP snooping function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable global IGMP snooping function	**ip igmp snooping**	Mandatory By default, the global IGMP snooping function is not enabled.
Enable the IGMP snooping function of the specified VLAN	**ip igmp snooping vlan** *vlan-id*	Mandatory By default, the IGMP snooping function is not enabled in the VLAN.

NOTE

- After enabling the global IGMP snooping function, you can enable the IGMP snooping function of the specified VLAN.

Configure IGMP snooping Version

The configured IGMP snooping version and the processing rules of the IGMP protocol packets are as follows:

The configured IGMP snooping version is V3 and the device can process IGMP protocol packets of V1, V2 and V3;

The configured IGMP snooping version is V2 and the device can process the IGMP protocol packets of V1 and V2 and does not process V3 protocol packets, but make V3 protocol packets flood in VLAN.

The configured IGMP snooping version is V1 and the device can process the IGMP protocol packets of V1 and does not process V2 or V3 protocol packets, but make V2 and V3 protocol packets flood in VLAN.

Table 493 Configure IGMP snooping version

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IGMP snooping version	**ip igmp snooping vlan** *vlan-id* **version** *version-number*	Optional By default, the IGMP snooping version is 2.

Enable IGMP snooping IP Forwarding

Usually, IGMP snooping forwards the multicast service packet in VLAN according to the destination MAC address. After configuring IGMP snooping IP forwarding, IGMP snooping forwards multicast service packets in VLAN according to the multicast source IP address and multicast destination IP address.

Table 494 IGMP snooping IP forwarding

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable global L2 multicast IP forwarding	**ip igmp snooping ipmc l2-forwarding**	Mandatory By default, MAC forwarding function of global IGMP snooping L2 multicast is enabled.
Enable L2 multicast IP forwarding function in the specified VLAN	**ip igmp snooping vlan** *vlan-id* **ipmc l2-forwarding**	Mandatory By default, MAC forwarding function of IGMP snooping L2 multicast in VLAN is enabled.

49.2.2 Configure IGMP snooping Querier *-B -S -E -A*

If there is no L3 multicast device in the network, it cannot realize the related functions of the IGMP querier. To solve the problem, you can configure the IGMP snooping querier on the L2 multicast device to realize the IGMP querier function so that L2 multicast device can set up and maintain multicast forwarding entry, so as to forward multicast service packets normally.

Configuration Conditions

Before configuring the basic functions of IGMP snooping querier, first complete the following task:

- Enable global and VLAN IGMP snooping function

Enable IGMP snooping Querier

You should first enable the IGMP snooping querier function so that the configuration of the other features of the querier can take effect.

Table 495 Enable IGMP snooping querier

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable the IGMP snooping querier	**ip igmp snooping vlan** *vlan-id* **querier**	Mandatory By default, the IGMP snooping querier of the specified VLAN is not enabled.

Configure Querier IP Address

The querier configured with IP address takes part in the election of the IGMP querier in VLAN and the querier fills the IP address in the source IP address field of the sent IGMP group query packet.

Table 496 Configure querier IP address

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP address of the querier	**ip igmp snooping vlan** *vlan-id* **querier address** *ip-address*	Mandatory By default, the querier IP address of the specified VLAN is not configured.

NOTE

- When the querier IP address is not configured, the default source IP address of the querier is 0.0.0.0, but the querier does not send the IGMP group query packet with source IP address 0.0.0.0.

Configure Query Interval of General Group

IGMP querier periodically sends the query packets of the general group to maintain the group member relation. You can modify the interval of sending the IGMP general group query packets according to the actuality of the network. For example, if the configured general group query interval is long, it can reduce the number of the IGMP protocol packets in the network, avoiding the network congestion.

Table 497 Configure query interval of general group

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure query interval of general group	**ip igmp snooping vlan** *vlan-id* **querier query-interval** *interval-value*	Optional By default, the query interval of the general group is 125s.

NOTE

- In the same VLAN, the configured query interval of the general group should be larger than the maximum response time. Otherwise, the configuration cannot succeed.

Configure Max. Response Time

The general group query packet sent by IGMPv2 querier contains the maximum response time field. The multicast receiver sends the member report packets within the maximum response interval. If the multicast receiver does not send the member report packets within the maximum response time, the device regards that the subnet does not have the receiver of the multicast group and then deletes the multicast group information at once.

Table 498 Configure the maximum response time

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the maximum response time	**ip igmp snooping vlan** *vlan-id* **querier max-response-time** *time-value*	Optional By default, the maximum response time is 10s.

NOTE

- In one VLAN, the configured maximum response time should be smaller than the query interval of the general group. Otherwise, the configuration cannot succeed.

Configure Query Interval of Specified Group

When the IGMP querier receives the leave packet of one multicast group, it sends the query packet of the specified group to query the segment for the multicast group, so as to know whether the subnet has the member of the multicast group. If not receiving the member report packet of the multicast group after waiting for "maximum response time", delete the information of the multicast group.

Table 499 Configure query interval of specified group

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure query interval of specified group	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *interval-value*	Optional By default, the query interval of the specified group is 1000 ms.

Configure Fast Leave

If the device receives the leave packet of one multicast group after configuring fast leave, the device does not send the query packet of the specified group to the port any more and the information of the multicast group is deleted at once.

Table 4910 Configure fast leave

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the fast leave	**ip igmp snooping vlan** *vlan-id* **immediate-leave**	Mandatory By default, the fast leave function of the specified VLAN is not enabled.

NOTE

- There are multiple receivers of the same multicast group in the device port at the same time. When the port receives the IGMP leave packet of the multicast group sent by one receiver and if fast leave is configured in the VLAN of the device port, the multicast services of the other receivers are interrupted.

49.2.3 Configure IGMP snooping Router Port *-B -S -E -A*

IGMP snooping router port is the port receiving IGMP group query packets or multicast routing protocol packets. When the device receives the IGMP member report or leave packet, forward the packet via

IGMP snooping router port. In this way, the upper-connected router can maintain the IGMP member relation table correctly.

IGMP snooping router port can be dynamically learned or configured manually. IGMP snooping dynamic router port refreshes the age time by regularly receiving the IGMP group query packets or multicast routing protocol packets. IGMP snooping static router port does not age.

Configuration Conditions

Before configuring the IGMP snooping router port functions, first complete the following tasks:

- Enable global and VLAN IGMP snooping function
- Add port member in VLAN

Configure IGMP snooping Static Router Port

After configuring IGMP snooping static router port, the device can forward the IGMP protocol packet via the port even the port does not receive the IGMP group query packet or multicast routing protocol packet. It can prevent the problem that the router port ages because the services of the upper-connected L3 multicast device are interrupted.

Table 4911 Configure IGMP snooping static router port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IGMP snooping static router port	**ip igmp snooping vlan** *vlan-id* **mrouter** { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* }	Mandatory By default, the IGMP snooping static router port is not configured.

Configure Age Time of IGMP snooping Dynamic Router Port

If the configured age time of the IGMP snooping dynamic router port is longer, it can prevent the problem that the router port of the upper-connected L3 multicast device is aged fast because of the service interruption.

Table 4912 Configure age time of IGMP snooping dynamic router port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure age time of IGMP snooping dynamic router port	**ip igmp snooping vlan** *vlan-id* **timer router-port expiry** *expiry-value*	Optional By default, the age time of IGMP snooping dynamic router port is 255s.

49.2.4 Configure IGMP snooping TCN Event -B -S -E -A

Configuration Conditions

Before configuring the IGMP snooping TCN event function, first complete the following task:

- Enable global and VLAN IGMP snooping function

Enable fast convergence

When the network topology changes, generate the TCN event and the STP root port actively sends the global IMGP leave packets (group address: 0.0.0.0) to request the IGMP querier to send the general group query packet, reaching the fast convergence.

After enabling IGMP snooping TCN event fast convergence, non-STP root port also actively sends the global IGMP leave packet (group address: 0.0.0.0), reaching the fast convergence.

Table 4913 Enable fast convergence

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable fast convergence	**ip igmp snooping tcn query solicit**	Mandatory By default, the fast convergence is not enabled in the TCN event.

Configure Query Interval of TCN Event

When the TCN event happens, IGMP snooping querier sends the general group query according to the TCN event query interval.

Table 4914 Configure query interval of TCN event

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the query interval of the TCN event	**ip igmp snooping vlan** *vlan-id* **querier tcn query interval** *interval-value*	Optional By default, the query interval of the TCN event is 31s.

Configure Query Times of TCN Event

When the TCN event happens, IGMP snooping querier sends the general group query according to the query interval of the TCN event. After the sending times reaches the configured query times of the TCN event, restore to the query interval of the general group.

Table 4915 Configure query times of TCN event

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the query times of the TCN event	**ip igmp snooping vlan** *vlan-id* **querier tcn query count** *count-number*	Optional By default, the query times of the TCN event is 2.

49.2.5 Configure IGMP snooping Policy *-B -S -E -A*

IGMP snooping policy is mainly used to control the receiver on the port, so as to control the multicast flow and limit the receiver action. In the setup L2 multicast flow forwarding environment, you also can apply the IGMP snooping policy.

Configuration Conditions

Before configuring the IGMP snooping policy, first complete the following task:

- Enable global and VLAN IGMP snooping function

Configure Port Filter Rule

When the receiver hopes to get the multicast service, actively initiate the IGMP member report packet and the device judges according to the applied port filter rule in the port: refuse the user to add the destination multicast group; permit the user to add the destination multicast group; limit the times and time of the user adding the destination multicast group.

Table 4916 Configure port filter rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the IGMP profile configuration mode	**ip igmp profile** *profile-id*	-
Configure the range of the refused multicast group	**deny** { **all** | *low-ip-address* [*high-ip-address*] }	Optional By default, the range of the refused multicasts group is not configured.

Step	Command	Description
Configure the range of the permitted multicast group	**permit** { **all** | *low-ip-address* [*high-ip-address*] }	Optional By default, the range of the permitted multicasts group is not configured.
Configure the preview multicast group rule	**preview** { **all** | *low-ip-address* [*high-ip-address*] | **count** *count-number* | **interval** *interval-time* | **time** *time-duration* }	Optional By default, the preview multicast group rule is not configured.
Return to global configuration mode	**exit**	-
Enter L2 Ethernet interface configuration mode	**interface** *interface-name*	You should select one of them. After entering L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port; after entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
In the port, apply the IGMP port filter rule	**ip igmp filter** *profile-number*	Mandatory By default, the IGMP port filter rule is not applied in the port.

NOTE

- Multicast group address can only be in one IGMP profile filter rule: deny, permit and preview. The new rule covers the old rule.
- Reset period of preview times > preview time × preview times + preview interval × (preview time – 1).

Configure Maximum Number of Port Multicast Groups

The maximum number of the port multicast groups can limit the number of the multicast groups the receiver is added to.

Table 4917 Maximum number of port multicast groups

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2 Ethernet interface configuration mode	**interface** *interface-name*	You should select one of them. After entering L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port; after entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure maximum number of the multicast groups in the port	**ip igmp max-groups** *number*	Optional By default, the maximum number of the multicast groups the port can dynamically be added to is 500.

Configure Upper-limitation Policy of Port Multicast Groups

When the number of the multicast groups the receiver is added to exceeds the configured maximum number of the multicast groups: If the upper-limitation policy of the port multicast group is replace, the new added multicast group on the device automatically replaces the existing multicast group; if the upper-limitation policy of the port multicast group is refuse, refuse the new added multicast group.

Table 4918 Configure upper-limitation policy of port multicast group

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2 Ethernet interface configuration mode	**interface** *interface-name*	You should select one of them.

Step	Command	Description
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	After entering L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port; after entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure the upper-limitation policy of the port multicast group	**ip igmp max-groups action** { **deny** | **replace** }	Optional By default, the processing action after the number of the multicast groups the port is dynamically added to reaches the maximum is refuse.

49.2.6 Configure IGMP Snooping Proxy *-B -S -E -A*

When there are many receivers of the multicast group in the network, to reduce the number of the IGMP member report and leave packets received by the upstream multicast device and reduce the system cost effectively, you can configure IGMP snooping proxy on the device.

IGMP snooping proxy deputizes the downstream receiver to send the IGMP member report packets and leave packets to the upstream device and also can answer the IGMP group query packet sent by the upstream multicast device and then send the IGMP group query packet to the downstream device.

Configuration Conditions

Before configuring the IGMP snooping proxy function, first complete the following task:

- Enable global and VLAN IGMP snooping function

Configure IGMP Snooping Proxy

Table 4919 Configure IGMP snooping proxy

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IGMP snooping proxy	**ip igmp snooping proxy vlan** *vlan-id* **upstream** { **interface** *interface-*	Mandatory

Step	Command	Description
	name | **link-aggregation** *link-aggregation-id* }	By default, IGMP agent port is not configured in VLAN.

49.2.7 IGMP snooping Monitoring and Maintaining *-B -S -E -A*

Table 4920 IGMP snooping monitoring and maintaining

Command	Description
clear ip igmp snooping groups [**grp-addr** *ip-address* | **vlan** *vlan-id* [**grp-addr** *ip-address-in-vlan*]]	Clear the IGMP snooping group information
clear ip igmp snooping statistics { **vlan** *vlan-id* } [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Clear the IGMP protocol packet statistics information
show ip igmp snooping proxy member database [**vlan** *vlan-id*]	Display the IGMP snooping proxy member database information
show ip igmp snooping proxy special query source-list [**vlan** *vlan-id*]	Display the source list of the specified source query received by IGMP snooping proxy
show ip igmp snooping proxy upstream [**vlan** *vlan-id*]	Display the IGMP snooping proxy running information
show ip igmp snooping debugging	Display the IGMP snooping debugging status information
show ip igmp snooping egress_table	Display the L2 forwarding table of IGMP snooping
show ip igmp snooping groups [[**vlan** *vlan-id*] **grp-addr** *ip-address*]	Display the IGMP snooping multicast group information
show ip igmp snooping groups [**vlan** *vlan-id*] **count**	Display the number of IGMP snooping multicast groups
show ip igmp snooping groups detail [[**vlan** *vlan-id*] **grp-addr** *ip-address*]	Display the details of IGMP snooping multicast group

Command	Description
show ip igmp snooping interface statistics	Configure the statistics information of the multicast groups the IGMP snooping port is added to
show ip igmp snooping l3_ip_table	Display the L3 IP forwarding table of IGMP snooping
show ip igmp snooping mcast_table	Display the forwarding table of IGMP snooping
show ip igmp snooping mrouter [**vlan** *vlan-id*]	Display the IGMP snooping router port information
show ip igmp snooping querier [**vlan** *vlan-id*]	Display the IGMP snooping querier information
show ip igmp snooping statistics [**vlan** *vlan-id*]	Display the IGMP packet statistics information of the IGMP snooping port
show ip igmp snooping [**vlan** *vlan-id* [**info**]]	Display the IGMP snooping information
show multicast control [**all-info |** **interface** *interface-name* **| link-aggregation** *link-aggregation-id*]	Display the information of the L2 multicast control

49.3 Typical Configuration Example of IGMP snooping

49.3.1 Configure IGMP snooping *-B -S -E -A*

Network Requirements

- Device1 configures the multicast route protocol; Device2 enables IGMP snooping; PC1 and PC2 are the receivers of the multicast service; PC3 is the receiver of the non-multicast service.
- Multicast Server sends the multicast service packets; PC1 and PC2 can receive the multicast service packets; PC3 cannot receive the multicast service packet.

Network Topology

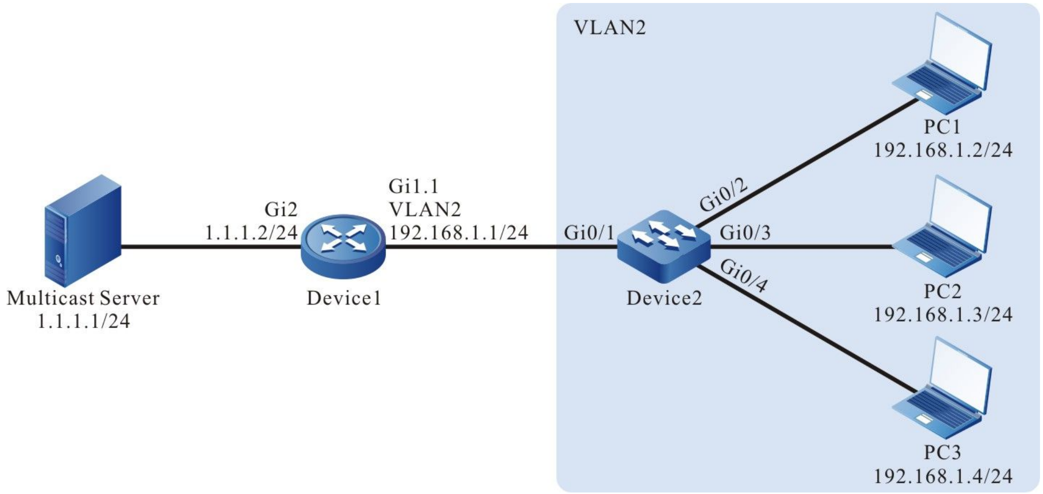


Figure 491 Network topology of IGMP snooping

Configuration Steps

Step 1: Device1 configure the interface IP address and enables the multicast route protocol. (omitted)

Step 2: Configure Device2.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of the port gigabitethernet0/2-gigabitethernet0/4 on Device2 as Access, permitting the services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Trunk, permitting the services of VLAN2 to pass; PVID is configured as 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable dropping unknown multicast in VLAN2.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Enable IGMP snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
```

Step 3: Check the result.

# PC1 and PC2 send IGMPv2 member report packet to add multicast group 224.1.1.1.

#View the multicast member table of Device2.

```
Device2#show ip igmp snooping groups
VLAN ID  Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime

_______  _________________ _____________ _______ _____________      _________
2        gi0/2        224.1.1.1    00:03:26  192.168.1.3  stopped        00:00:55
2        gi0/3        224.1.1.1    00:03:44  192.168.1.4  stopped        00:00:40
```

#Multicast Server sends the multicast service packet with destination address 224.1.1.1; PC1 and PC2 can correctly receive the multicast service packet; PC3 cannot receive the multicast service packet.

49.3.2 Configure Multicast Receiving Control *-B -S -E -A*

Network Requirements

- Device1 configures multicast routing protocol.
- Device2 enables IGMP snooping, configures multicast receiving control and applies to the corresponding port.
- Multicast Server sends the multicast service packet; PC1 and PC2 can receive the multicast service packet.

Network Topology

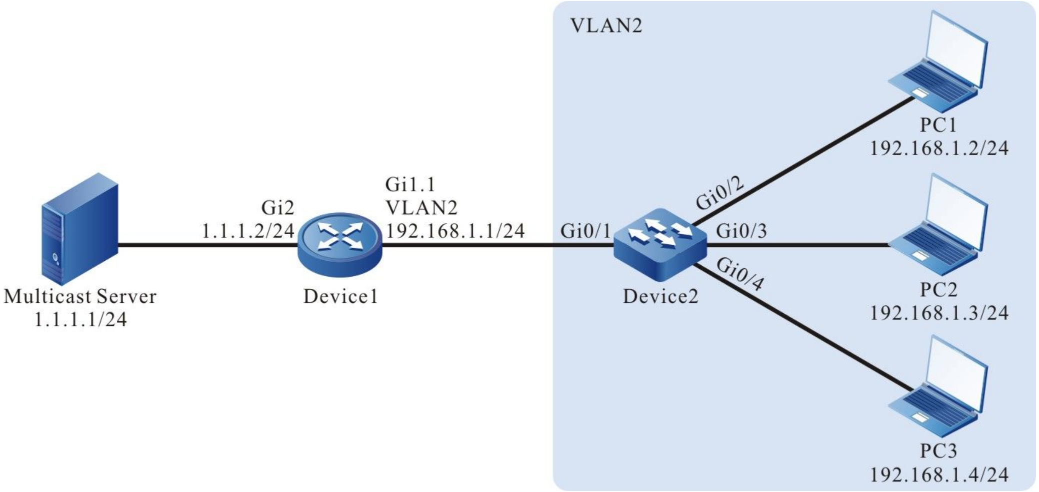


Figure 492 Network topology of configuring multicast receiving control

Configuration Steps

Step 1: Device1 configures the interface IP address and enables the multicast route protocol. (omitted)

Step 2: Configure Device2.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of the port gigabitethernet0/2-gigabitethernet0/4 on Device2 as Access, permitting the services of VLAN2 to pass.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Trunk, permitting the services of VLAN2 to pass; PVID is configured as 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable IGMP snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
```

#Configure multicast receiving control policy profile1, permits to add multicast group 224.1.1.1 and apply to port gigabitethernet0/2.

```
Device2(config)#ip igmp profile 1
Device2(config-igmp-profile)#permit 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#ip igmp filter 1
Device2(config-if-gigabitethernet0/2)#exit
```

#Configure multicast receiving control policy profile2, preview multicast group 224.1.1.1 and apply to port gigabitethernet0/3.

```
Device2(config)#ip igmp profile 2
Device2(config-igmp-profile)#preview 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#ip igmp filter 2
Device2(config-if-gigabitethernet0/3)#exit
```

#Configure multicast receiving control policy profile3, refuse adding to multicast group 224.1.1.1 and apply to port gigabitethernet0/4.

```
Device2(config)#ip igmp profile 3
Device2(config-igmp-profile)#deny 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/4
Device2(config-if-gigabitethernet0/4)#ip igmp filter 3
Device2(config-if-gigabitethernet0/4)#exit
```

Step 3: Check the result.

#PC1, PC2 and PC3 send IGMPv2 member report packet to add to multicast group 224.1.1.1.

#View multicast member table of Device2.

```
Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 2 groups

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
```

```
2      gi0/2         224.1.1.1     00:04:19  192.168.1.2 stopped             00:00:01
2      gi0/3         224.1.1.1     00:04:19  192.168.1.3 stopped             00:00:01
```

PC1 and PC2 can add to multicast group 224.1.1.1; PC3 does not add to multicast group 224.1.1.1.

# Multicast Server sends the multicast service packet with destination address 224.1.1.1.

PC1 and PC2 can correctly receive the multicast service packet; PC3 cannot receive the multicast service packet.

#After waiting for 10s, view the multicast member table of Device2 and multicast receiving control information of gigabitethernet0/3.

```
Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total1 group

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime

2      gi0/2         224.1.1.1     00:04:10  192.168.1.2 stopped             00:00:10
Device2#show multicast control interface gigabitethernet 0/3
ip multicast control gigabitethernet0/3 vlan 2 information
--------------------------------------------
profile: 2
group right information:
 preview: 224.1.1.1
preview information:
  preview count: 3
  preview count remain: 2
  preview time: 10 (s)
  preview interval: 60 (s)
group information:
  group: 224.1.1.1
    uptime: 00:00:10
    next preview time remain: 00:00:60
```

After the preview time of port gigabitethernet0/3 arrives (after 10s), the group member entry is deleted; PC1 can correctly receive the multicast service packet; PC2 and PC2 cannot receive the multicast service packet.

49.3.3 Configure IGMP Snooping Proxy *-B -S -E -A*

Network Requirements

- Device1 configures multicast routing protocol.
- Device2 enables IGMP snooping and GMP snooping proxy.
- Multicast Server sends the multicast service packet; PC1, PC2, and PC3 can correctly receive the multicast service packet.

Network Topology

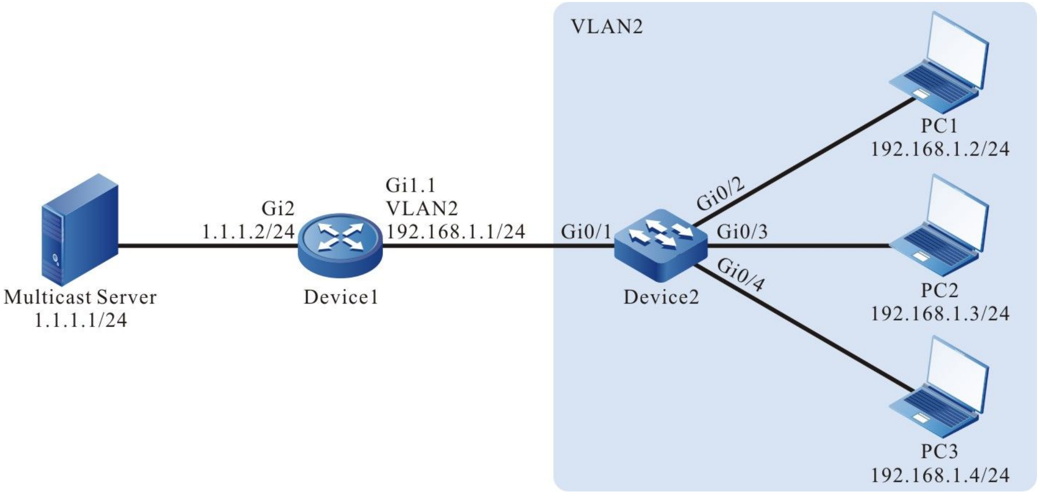


Figure 493 Network topology of configuring IGMP snooping proxy

Configuration Steps

Step 1: Device1 configures the interface IP address and enables the multicast route protocol.

```
Device1#configure terminal
Device1(config)#ip multicast-routing
Device1(config)#interface gigaethernet1.1
Device1(config-if-gigaethernet1.1)# ip address 192.168.1.1 255.255.255.0
Device1(config-if-gigaethernet1.1)# encapsulation dot1q 2
Device1(config-if-gigaethernet1.1)# ip pim sparse-mode
Device1(config-if-gigaethernet1.1)# exit
Device1(config)#interface gigaethernet2
Device1(config-if-gigaethernet2)# ip address 1.1.1.2 255.255.255.0
Device1(config-if-gigaethernet2)# ip pim sparse-mode
Device1(config-if-gigaethernet2)# exit
```

Step 2: Configure Device2.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of the port gigabitethernet0/2-gigabitethernet0/4 on Device2 as Access, permitting the services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Trunk, permitting the services of VLAN2 to pass; PVID is configured as 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable IGMP snooping in VLAN2; configure IGMP snooping querier address as 192.168.1.254.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 2 querier
Device2(config)#ip igmp snooping vlan 2 querier address 192.168.1.254
```

#Configure IGMP snooping proxy.

```
Device2(config)#ip igmp snooping proxy vlan 2 upstream interface gigabitethernet 0/1
Device2(config)#exit
```

Step 3:   Check the result.

#PC1, PC2 and PC3 successively sends IGMPv2 member report packets to add to multicast group 224.1.1.1.

#View the IGMP snooping proxy information of Device2.

```
Device2#show ip igmp proxy upstream vlan 2
vlan 2 proxy upstream information:
------------------------------
upstream interface                    : gi0/1
upstream querier compatmode version     : 2
upstream querier address              : 192.168.1.1
upstream querier query interval         : 125s
upstream querier query response interval: 10s
upstream querier LMQI                 : 1s
upstream querier LMQC                 : 2
upstream querier robustness variable    : 2
upstream querier present timer          : 00:02:50
upstream V1 querier present timer       : stopped
upstream V2 querier present timer       : 00:02:55
```

#View multicast member table of Device2 and IGMP snooping proxy member database.

```
Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 3 groups

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
_____________________________________________________ __________________________
2       gi0/2          224.1.1.1     00:04:09  192.168.1.2 stopped             00:00:14
2       gi0/3          224.1.1.1     00:04:09  192.168.1.3 stopped             00:00:11
2       gi0/4          224.1.1.1     00:04:12  192.168.1.4 stopped             00:00:07
```

You can see that PC1, PC2 and PC3 add to multicast group 224.1.1.1.

```
Device2#show ip igmp snooping proxy member database vlan 2
IGMP Snooping Proxy Member Database Table
Total 1 group

VLAN ID  Group Address    Mode     Source Address
-------  ---------------  -------  ---------------
2        224.1.1.1        EXCLUDE  *
```

#View multicast member table of Device1.

```
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address    Interface          Uptime   Expires  Last Reporter   V1 Expires
224.1.1.1        gigaethernet1.1    00:00:15 00:04:11 192.168.1.2      stopped
```

You can see that when PC adds to multicast group 224.1.1.1, Device2 can only forward the first IGMPv2 member report packet to Device1 and the other are all dropped.

#Multicast Server sends the multicast service packet with destination address 224.1.1.1; PC1, PC2 and PC3 can correctly receive the multicast service packet.

#PC1 and PC2 send IGMPv2 leave packet to leave multicast group 224.1.1.1.

```
Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 1 group

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
____________________________________________________________________________________________
_
2      gi0/4         224.1.1.1     00:03:54 192.168.1.4  stopped           00:06:37
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address    Interface          Uptime   Expires  Last Reporter   V1 Expires
224.1.1.1       gigaethernet1.1     00:06:48 00:03:48 192.168.1.2       stopped
```

After PC1 and PC2 leave multicast group 224.1.1.1, PC3 does not leave the multicast group, so there is still group member PC3 in the multicast member table. Therefore, Device2 does not send the leave packet of the multicast group to Device1.

#PC3 sends the IGMPv2 leave packet to leave multicast group 224.1.1.1; view multicast member table of Device2 and Device1.

```
Device2#show ip igmp snooping groups
```

You can see that there is no multicast member table on Device2.

```
Device1#show ip igmp groups
```

There is no multicast member on Device1. When the last group member PC3 leaves the multicast group, Device2 sends the leave packet of the multicast group to Device1.

#PC1, PC2 and PC3 cannot receive the multicast service packet.

50 IPv4 Multicast Infrastructure

50.1 Overview of IPv4 Multicast Infrastructure

IPv4 multicast infrastructure is the foundation on which IP multicast protocol runs, it is a common component of all multicast protocols. No matter what multicast routing protocol is run, the IP multicast forwarding function has to be enabled first for the Device to be able to forward multicast business message.

50.2 IPv4 Multicast Basic Function Configuration

Table 50-1 IPv4 Multicast Basic Function Configuration List

Configuration task	
Enable IP multicast forwarding	Enable IP multicast forwarding
Configure IP multicast forwarding rules	Configure multicast forwarding management border
	Configure multicast forwarding table entry limit

NOTE

- L3 ethernet interface does not support IP multicast forwarding rules function.

50.2.1 Enable IP Multicast Forwarding *-E -A*

Configuration Conditions

None

Enable IP Multicast Forwarding

Enable IP multicast forwarding function, which is a prerequisite for safeguarding the normal operation of forwarding multicast business.

Table 50-2 Enable IP Multicast Forwarding

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable IP multicast forwarding	**ip multicast-routing** [**vrf** *vrf-name*]	Required Enable IP multicast forwarding. By default, IP multicast forwarding is not enabled

50.2.2 Configure IP Multicast Forwarding Rules *-E -A*

Configuration Conditions

The following tasks have to be completed first before configuring interface's multicast forwarding management border:

- Configure interface's IP address to make neighboring node network layers reachable;
- Enable IP multicast forwarding ;
- Configure multicast routing protocol.

Configure Multicast Forwarding Management Border

After the configuration of management border, device can filter multicast business messages. Multicast business messages that do not match the access list rules will not be forwarded from the interface.

Table 50-3 Configure Multicast Forwarding Management Border

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure multicast forwarding management border	**ip multicast boundary** { *access-list-number* | *access-list-name* }	Required By default, multicast forwarding management border is not configured

Configure Multicast Forwarding Table Entry Time-Out

Configure multicast forwarding table entry time-out, upon the expiry of which table entries will be deleted or subjected to other operations according to their identifier.

Table 50-4 Configure Multicast Forwarding Table Entry Time-Out

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure multicast forwarding table entry time-out	**ip multicast mrt-timer** *timevalue*	Optional By default, multicast forwarding table entry time-out is 180S

Configure Multicast Forwarding Table Entry Limit

Configure maximum limit for multicast forwarding table entries, beyond which limit new multicast forwarding entry will not be created.

Table 50-5 Configure Multicast Forwarding Table Entry Limit

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure multicast forwarding table entry limit	**ip multicast route-limit** *number-value* [**vrf** *vrf-name*]	Optional By default, multicast forwarding table's maximum number of entries is 6144. The range of get values can be adjusted depending on the system's working mode.

50.2.3 Basic Monitoring and Maintenance of IPv4 Multicast *-E -A*

Table 50-6 Basic Monitoring and Maintenance of IPv4 Multicast

Command	Description
clear ip mcache [**source** *source-ip-address*] [**group** *group-ip-address*] [**all | vrf** *vrf-name*]	Erase multicast routing table entries
show ip mcache [**source** *source-ip-address*] [**group** *group-ip-address*] [**vrf** *vrf-name*]	Display multicast routing table information
show ip mnhp [[**vrf** *vrf-name*] | [**vlan** *vlan-id*]]	Display multicast next hop information
show ip mvif [**vrf** *vrf-name*]	Display multicast virtual interface information
show ip mvrf	Display multicast VRF information

51 IGMP

51.1 IGMP Overview

Internet Group Management Protocol (IGMP), a member of the TCP/IP protocol family responsible for management of IP multicast members, is used to establish and maintain multicast group membership between IP host and its directly neighboring multicast device.

There are 3 versions of IGMP, currently IGMPv2 is the most extensively used version. IGMP v2 has three types of messages: query messages, membership report messages and leave group messages.

Query messages are divided into general query messages and group-specific query message. Device uses general query messages to find out the members of the Direct Interconnection Network and uses group-specific query messages to find out whether the Direct Interconnection Network has a member of certain designated group.

Membership report messages: when a host wants to join in a multicast group, the host will immediately send a membership report to the multicast group it wants to join. When the host receives a query message, it will also send a membership report.

Leave group messages: when the host leaves a multicast group, it sends a leave group report. When the Device receives the leave group message, it sends a group-specific query to determine whether a certain group is absent of any group member.

51.2 Configuration of IGMP Functions

Table 51–1 Functional Configuration List of IGMP

Configuration task	
Configure IGMP basic functions	Enable IGMP protocol
	Configure IGMP version
	Configure static group join
	Configure multicast group filter
	Configure SSM multicast group filter
Adjust and optimize IGMP network	Configure general group query time interval

Configuration task	
	Configure coefficient of robustness
	Configure maximum response time
	Configure group-specific query
	Configure other querier’s time-out
	Configure fast leave

NOTE

- L3 ethernet interface does not support IGMP function.

51.2.1 Configure IGMP Basic Functions *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of IGMP basic functions:

- Configure interface's network layer address to make neighboring node network layers reachable;

Enable IGMP Protocol

Table 51–2 Enable IGMP Protocol

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable IP multicast forwarding	**ip multicast-routing**	Required By default, IP multicast forwarding is not enabled
Enter the interface configuration mode	**interface** *interface-name*	-

Steps	Command	Description
Enable IGMP protocol	**ip pim sparse-mode**	Required By default, IGMP is not enabled. When multicast routing protocol is enabled for an interface, IGMP will automatically be enabled. Only after IGMP has been enabled will all IGMP related configurations take effect.

Configure IGMP Version

Table 51–3 Configure IGMP Version

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure IGMP version	**ip igmp version** *version-number*	Required By default, the IGMP version number is 2

NOTE

- In consideration of the differences in message structure and types between IGMP of different versions, it is recommended that IGMP of the same version shall be configured on all devices in the same subnet.

Configure Static Group Join

When an interface is configured a static group or source group, the Device will deem that the multicast group or source group under the interface has receiver.

Table 51–4 Configure Static Group Join

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure static group join	**ip igmp static-group** *group-ip-address* [*source-ip-address*]	Required By default, interface does not join in any multicast group or source group in static mode

Configure Multicast Group Filter

Interfaces that have been configured IGMP multicast group filter will filter membership reports in that network segment in accordance with ACL. Only ACL permitted membership reports will be processed and reports that are not permitted will be directly discarded. Information of existing multicast groups that are not permitted by ACL will be deleted immediately.

Table 51–5 Configure Multicast Group Filter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure IGMP multicast group filter	**ip igmp access-group** { *access-list-number* | *access-list-name* }	Required By default, multicast group filter is not configured

NOTE

- ip igmp access-group command only supports standard ACL.

Configure SSM Multicast Group Filter

Once IGMP accepted source group range is configured, the received source membership report will be filtered in order to limit the source group range served by the interface. For groups in PIM-SSM range, only those with IGMPv3 non(IS_EX, TO_EX) membership report permitted by access list (S, G) will be accepted

Table 51–6 Configure SSM Multicast Group Filter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure SSM multicast group filter	**ip igmp ssm-access-group** { *access-list-number* | *access-list-name* }	Required By default, SSM group members are not subjected to filtration limit.

NOTE

- ip igmp ssm-access-group command takes effect only when IGMPv3 is enabled on the interface.
- ip igmp ssm-access-group command takes effect only on source groups in the range of PIM SSM.
- ip igmp ssm-access-group command only supports extended ACL.

51.2.2 Adjust and Optimize IGMP Network *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the adjustment and optimization of IGMP network:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Enable IGMP protocol.

Configure General Group Query Time Interval

IGMP querier will periodically send general group query message to maintain group membership. The time interval for sending IGMP general group query messages may be revised depending on the actual conditions of the network.

Table 51–7 Configure General Group Query Time Interval

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure general group query time interval	**ip igmp query-interval** *interval-value*	Optional By default, the time interval for sending IGMP general group query messages is 125 seconds

NOTE

- The general query time intervals of devices on the same network segment should be as consistent as possible.
- The time interval for general group query must greater than the maximum response time, otherwise the configuration will not be successful.

Configure Coefficient of Robustness

Table 51–8 Configure Coefficient of Robustness

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure coefficient of robustness	**ip igmp robustness-variable** *variable-value*	Optional By default, the coefficient of

Steps	Command	Description
		robustness of IGMP querier is 2

NOTE

- Once coefficient of robustness has been configured, the following parameters will vary with the robustness parameter:
  1. Group member time-out = coefficient of robustness * general group query time interval + maximum response time;
  2. Other querier's time-out = coefficient of robustness * general query time interval + maximum response time/2;
  3. It can be inferred that the greater the coefficient of robustness, the longer the IGMP group member time-out and other querier's time-out; users have to set up this value depending on the network's actual conditions.

Configure Maximum Response Time

General group query messages sent by IGMPv2 querier contain a maximum response time field, receiver will send a membership report within the maximum response time interval.

Table 51–9 Configure Maximum Response Time

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure maximum response time	**ip igmp query-max-response-time** *seconds*	Optional By default, IGMP general group query's maximum response time is 10 seconds

Configure Group-Specific Query

When receiving the leave message of a multicast group, IGMP querier will send group-specific query message "number of group-specific queries" to query the multicast group on the network segment to find out whether there is still any member of the multicast group in the subnet. If, no membership report of the multicast group has been received upon expiry of "the last life cycle", the multicast group's information will be deleted.

Table 51–10 Configure Group-Specific Query

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure time interval for group queries	**ip igmp last-member-query-interval** *interval-value*	Optional By default, the time interval for sending group-specific query messages is 1 second
Configure number of group-specific queries	**ip igmp last-member-query-count** *count-value*	Optional By default, the sending number of group-specific query messages is 2

NOTE

- ip igmp last-member-query-interval command and ip igmp last-member-query-count command are invalid in IGMPv1, because IGMPv1 host does not send a leave message when leaving a multicast group.

Configure Other Querier’s Time-Out

In the same subnet, the Device that has smaller can be elected as querier, other devices are referred to as non-queriers. On non-queriers, a timer "other queriers' time-out" (timer "other-querier-present") will be set up for the querier. Non-queriers when receiving query message from the querier will refresh the timer. If the timer is time out, that means the current IGMP querier has expired and a new querier has to be re-elected.

Table 51–11 Configure Other Querier’s Time-Out

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure other querier's time-out	**ip igmp query-timeout** *seconds*	Optional By default, other querier's time-out is 255 seconds

NOTE

- If the configured other querier's time-out is less than the query time interval, querier in the network will change constantly.

Configure Fast Leave

If, the stub network segment of a network is connected only one host, which frequently switches multicast groups, then in order to reduce leave delay, multicast group fast leave can be configured on device.

If fast leave is configured, when device receives the leave message of a multicast group, it will check whether the multicast group belongs to the range of fast leave. If yes, the Device will no longer send group-specific query message to the network segment, and will delete the information of the multicast group immediately.

Table 51–12 Configure Fast Leave

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure fast leave multicast group's range	**ip igmp immediate-leave group-list** { *access-list-number* | *access-list-name* }	Required By default, the fast leave of multicast group is not allowed; this rule applies to IGMP v2

Steps	Command	Description
Configure fast leave source group range	**ip igmp sg-immediate-leave sg-list** { *access-list-number* | *access-list-name* }	Required By default, the fast leave of source group is not allowed; this rule applies to IGMP v3

51.2.3 Configure IGMP SSM Mapping *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of IGMP SSM mapping:

- Configure interface's network layer address to make neighboring node network layers reachable;
- Enable IGMP protocol.

Configure IGMP SSM Mapping

In PIM-SSM network, in order to provide PIM-SSM service to receiver that supporting IGMPv3, it is acceptable to configure IGMP SSM mapping function on the device.

The user may, depending on network receiver needs, configure IGMP SSM mapping rules. The rules permitted membership reports will be converted to IGMPv3 non(IS_EX, TO_EX) membership reports, the multicast source address of which is the source address specified by the IGMP SSM mapping rules.

Table 51-13 Configure IGMP SSM Mapping

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable IGMP SSM Mapping	**ip igmp ssm-map enable** [**vrf** *vrf-name*]	Required By default, IGMP SSM Mapping is not enabled
Configure IGMP SSM Mapping rules	**ip igmp ssm-map static** { *access-list-number* | *access-list-name* } *source-ip-address* [**vrf** *vrf-name*]	Required By default, there are no IGMP SSM Mapping rules

NOTE

- **ip igmp ssm-map static** command only supports standard ACL.

51.2.4 IGMP Monitoring and Maintenance *-E -A*

Table 51-14 IGMP Monitoring and Maintenance

Command	Description
clear ip igmp group [*group-ip-address*] [*interface-name*] [**vrf** *vrf-name*]	Erase IGMP multicast group information
clear ip igmp statistic interface *interface-name* [**vrf** *vrf-name*]	Erase IGMP message statistical information on interface
show ip igmp groups [[**static**] | [*interface-name*] [*group-ip-address*] [**detail**]] [**vrf** *vrf-name*]	Display IGMP multicast group information
show ip igmp interface [*interface-name*] [**vrf** *vrf-name*]	Display interface IGMP information
show ip igmp statistic interface *interface-name* [**vrf** *vrf-name*]	Display IGMP message statistical information

51.3 Example of IGMP Typical Configuration

51.3.1 Configure IGMP *-E -A*

Network Requirements

- The entire network runs PIM-SM protocol.
- Device1, Device2, and Receiver are in the same LAN, and Device2 is querier.
- Receiver is a receiver of Device1 and Device2 stub network.
- IGMPv2 runs between Device1 and Device2 and stub network.

Network Topology

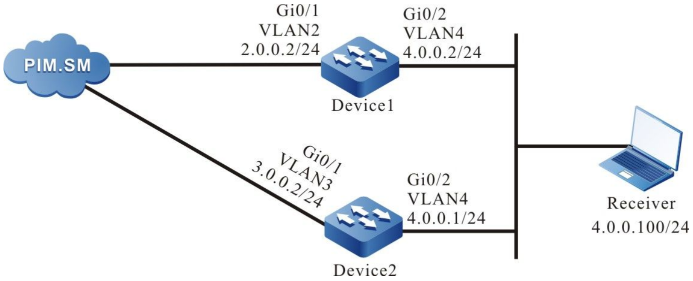


Figure 51-1 Networking Diagram - Configure IGMP

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Globally enable multicast forwarding, enable multicast protocol PIM-SM on interfaces.

#Configure Device1.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device1(config)#configure terminal
Device1(config)#ip multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device2(config)#configure terminal
Device2(config)#ip multicast-routing
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip pim sparse-mode
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
```

Step 3: Check the result.

#Check Device1 interface VLAN4's IGMP version information, querier election results.

```
Device1#show ip igmp interface vlan4
```

```
Interface vlan4 (Index 50331921)
 IGMP Active, Non-Querier (4.0.0.1, Expires: 00:02:15)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 4.0.0.2
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds configged, and 10 seconds is adopted
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

#Check Device2 interface VLAN4's IGMP version information, querier election results.

```
Device2#show ip igmp interface vlan4
Interface vlan4  (Index 50331921)
 IGMP Active, Querier (4.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 4.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

#Receiver sends an IGMPv2 membership report to join in the multicast group 225.1.1.1.

#Check Device1's multicast member list.

```
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address    Interface           Uptime      Expires     Last Reporter   V1 Expires  V2 Expires
225.1.1.1        vlan4    00:21:02   00:03:47    4.0.0.100        stopped
```

#Check Device2's multicast member list.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
```

```
Total 1 groups
Group Address    Interface            Uptime      Expires     Last Reporter   V1 Expires  V2 Expires
225.1.1.1        vlan4   00:21:02   00:03:47    4.0.0.100       stopped
```

NOTE

- The configuration of multicast protocol on interface automatically enables IGMP function; by default, IGMPv2 will run. Use command ip igmp version can configure the version of IGMP running on the interface.
- When multiple devices run IGMP in the same LAN, they will elect an IGMP querier, the devices with smaller IP address will be elected as the IGMP querier in the LAN.

51.3.2 Configure IGMP SSM Mapping *-E -A*

Network Requirements

- The entire network runs PIM-SSM protocol.
- Receiver1, Receiver2, Receiver3, and Device2 are in the same LAN.
- IGMPv3 runs between Device2 and stub network.
- The application of IGMP SSM mapping on Device2 renders Receiver2, Receiver3 can only receive multicast messages sent by Source1.

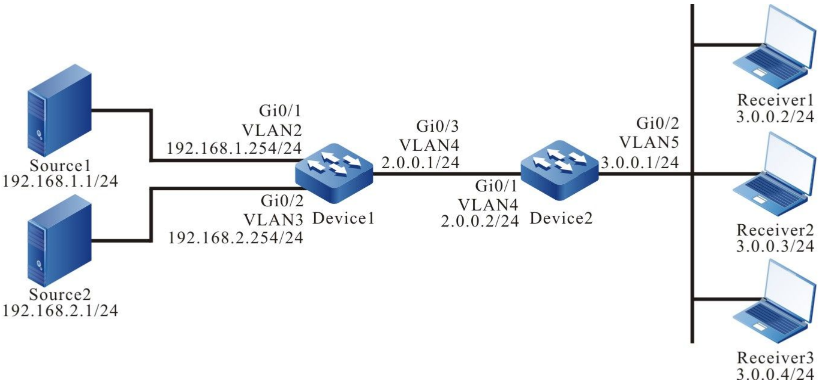


Figure 51-2 Networking Diagram - Configure IGMP SSM Mapping

Configuration Steps

Step 1: Configure IP addresses of the interfaces (omitted).

Step 2: Enable unicast routing protocol OSPF, so that all network devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
```

```
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Query the routing table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 00:16:05, vlan4
C   3.0.0.0/24 is directly connected, 00:06:36, vlan5
O   192.168.1.0/24 [110/2] via 2.0.0.1, 00:15:17, vlan4
O   192.168.2.0/24 [110/2] via 2.0.0.1, 00:00:51, vlan4
```

NOTE

- Device1's checking method is similar to that of Device2, the checking process is omitted here.

Step 3: Globally enable multicast forwarding, globally configure PIM-SSM, and SSM service’s multicast group range is 232.0.0.0/8. Enable multicast protocol PIM-SM on interfaces. Device2's interface vlan5 runs IGMPv3.

#Configure Device1.

Globally enable multicast forwarding, globally configure PIM-SSM, and enable multicast protocol PIM-SM on relevant interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#ip pim ssm default
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
```

```
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable multicast forwarding, globally configure PIM-SSM, and enable multicast protocol PIM-SM on relevant interfaces, interface vlan5 runs IGMPv3.

```
Device2(config)#ip multicast-routing
Device2(config)#ip pim ssm default
Device2(config)#interface vlan4
Device2(config-if-vlan40)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ip pim sparse-mode
Device2(config-if-vlan5)#ip igmp version 3
Device2(config-if-vlan5)#exit
```

#Check Device2's interface vlan5's IGMP information.

```
Device2#show ip igmp interface vlan5
Interface vlan5 (Index 50331921)
 IGMP Enabled, Active, Querier (3.0.0.1)
 Configured for version 3
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 3.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

Step 4: The enabling of IGMP SSM mapping and configuration of IGMP SSM mapping rules on Device2 make Receiver1, Receiver2 can only receive multicast messages sent by Source1.

#Configure Device2.

Enable IGMP SSM mapping, configure IGMP SSM mapping's multicast group range to 232.0.0.0~232.0.0.255, multicast source address is 192.168.1.1.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 232.0.0.0 0.255.255.255
```

```
Device2(config-std-nacl)#exit
Device2(config)#ip igmp ssm-map enable
Device2(config)#ip igmp ssm-map static 1 192.168.1.1
```

#Check Device2's IGMP SSM mapping rules.

```
Device2#show ip igmp ssm-map

 IGMP SSM-MAP Information : enable
 acl-name   source-addr
 --------------------------
1          192.168.1.1
```

Step 5: Check the result.

#Receiver1 sends an IGMPv3 membership report of designated source group to join in the multicast group232.1.1.1, the designated multicast source is 192.168.2.1; Receiver2 sends an IGMPv2 membership report to join in the multicast group 232.1.1.2; Receiver3 sends an IGMPv1 membership report to join in the multicast group 232.1.1.3.

#Both Source1 and Source2 send multicast message of multicast groups 232.1.1.1, 232.1.1.2, ,232.1.1.3.

#Check Device2's multicast member list.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 3 groups
Group Address    Interface        Uptime   Expires  Last Reporter   V1 Expires  V2 Expires
232.1.1.1        vlan5         01:28:45  stopped 3.0.0.2          stopped    stopped
232.1.1.2        vlan5         01:29:01  stopped 3.0.0.3          stopped    stopped
232.1.1.3        vlan5         01:29:16  stopped 3.0.0.4          stopped    stopped

Device2#show ip igmp groups detail
Interface:vlan5
Group:         232.1.1.1
Uptime:         01:30:44
Group mode:     Include
Last reporter:  3.0.0.2
TIB-A Count:    1
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
  192.168.2.1     01:30:44  00:03:39  stopped   Yes  R

Interface: vlan5
```

```
Group:          232.1.1.2
Uptime:         01:31:00
Group mode:     Include
Last reporter:  3.0.0.3
TIB-A Count:    1
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
  192.168.1.1     01:31:00  stopped   00:03:38  Yes  M

Interface: vlan5
Group:          232.1.1.3
Uptime:         01:31:15
Group mode:     Include
Last reporter:  3.0.0.4
TIB-A Count:    1
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
  192.168.1.1     01:31:15  stopped   00:03:42  Yes  M
```

#Check Device2's multicast routing table.

```
Device2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 3 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer



(192.168.2.1, 232.1.1.1)
Up time: 01:32:51
KAT time: 00:03:24
RPF nbr: 2.0.0.1
RPF idx: vlan4
SPT bit: TRUE
Flags:
  JOIN DESIRED
```

```
Upstream State: JOINED
  Local interface list:
    Vlan5
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    Vlan5
  Packet count 19868613

(192.168.1.1, 232.1.1.2)
Up time: 01:33:07
KAT time: 00:03:24
RPF nbr: 2.0.0.1
RPF idx: vlan4
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    Vlan5
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    Vlan5
  Packet count 19873645

(192.168.1.1, 232.1.1.3)
Up time: 01:33:22
KAT time: 00:03:24
RPF nbr: 2.0.0.1
RPF idx: vlan4
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    Vlan5
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
        Vlan5
       Packet count 19873645
```

#Receiver1 can only receive multicast message sent by Source2, Receiver2 and Receiver3 can only receive multicast message sent by Source1.

NOTE

- Device1's checking method is similar to that of Device2, the checking process is omitted here.
- IGMP SSM mapping has to be used in conjunction with PIM-SSM. The multicast group range in IGMP SSM mapping rules has to fall in the multicast group range of PIM-SSM. IGMP SSM mapping is mainly for providing receiver hosts that run IGMPv1 or IGMPv2 and cannot be upgraded to IGMPv3 with support to SSM model.
- IGMP SSM mapping is invalid for IGMPv3 membership reports.

51.3.3 Configure IGMP Static Join Group *-E -A*

Network Requirements

- The entire network runs PIM-SM protocol.
- Receiver is a receiver in Device stub network.
- IGMPv2 runs between Device and stub network.
- Device's interface vlan3 joins in multicast group 225.1.1.1 in static join group mode.

Network Topology

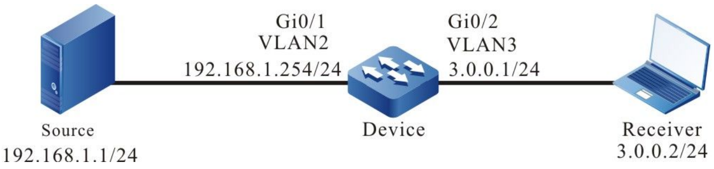


Figure 51-3 Networking Diagram - Configure IGMP Static Join Group

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Globally enable multicast forwarding, enable multicast protocol PIM-SM on interfaces.

#Configure Device.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device(config)#configure terminal
Device(config)#ip multicast-routing
Device(config)#interface vlan2
Device(config-if-vlan2)#ip pim sparse-mode
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ip pim sparse-mode
Device(config-if-vlan3)#exit
```

#Check Device's interface vlan3's IGMP information.

```
Device#show ip igmp interface vlan3
Interface vlan3 (Index 50331921)
 IGMP Active, Querier (3.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 3.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

Step 3: Device's interface vlan3 joins in multicast group 225.1.1.1 in static join group mode.

#Configure Device.

Device's interface vlan3 is configured static multicast group 225.1.1.1.

```
Device(config)#interface vlan3
Device(config-if-vlan3)#ip igmp static-group 225.1.1.1
Device(config-if-vlan3)#exit
```

Step 4: Check the result.

#Source sends multicast message of multicast group 225.1.1.1.

#Check Device's multicast member list.

```
Device#show ip igmp groups
IGMP Static Group Membership
Total 1 static groups
Group Address    Source Address   Interface
225.1.1.1        0.0.0.0          vlan3
```

#Check Device's multicast routing table .

```
Device#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:08:12
RP: 0.0.0.0
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    vlan3
  Joined interface list:
  Asserted interface list:


(192.168.1.1, 225.1.1.1)
Up time: 00:07:24
KAT time: 00:02:22
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
  COULD REGISTER
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    register_vif0
  Asserted interface list:
```

```
  Outgoing interface list:
    register_vif0
    vlan3
  Packet count 8646421

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:07:24
RP: 0.0.0.0
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
vlan3
```

#Receiver can receive the multicast message of multicast group 225.1.1.1 sent by Source.

51.3.4 Configure IGMP Multicast Group Filter *-E -A*

Network Requirements

- The entire network runs PIM-SM protocol.
- Receiver is a receiver of Device's stub network.
- IGMPv2 runs between Device and stub network.
- Device's interface vlan3 filters the multicast groups, Receiver is allowed to join in multicast groups in the range of 225.1.1.0~225.1.1.255.

Network Topology

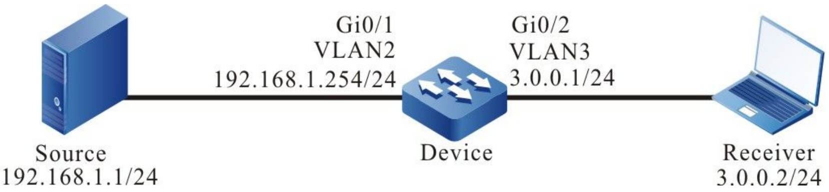


Figure 51-4 Networking Diagram - Configure IGMP Multicast Group Filter

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Globally enable multicast forwarding, enable multicast protocol PIM-SM on interfaces.

#Configure Device.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device(config)#configure terminal
Device(config)#ip multicast-routing
Device(config)#interface vlan2
Device(config-if-vlan2)#ip pim sparse-mode
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ip pim sparse-mode
Device(config-if-vlan3)#exit
```

#Check Device's interface vlan3's IGMP information.

```
Device#show ip igmp interface vlan3
Interface vlan3 (Index 50331921)
 IGMP Enabled, Active, Querier (3.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 3.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

Step 3: Configure multicast group filter on Device's interface vlan3.

#Configure Device.

Configure multicast group filter on Device's interface vlan3, the multicast group range that Receiver is allowed to join is 225.1.1.0~225.1.1.255.

```
Device(config)#ip access-list standard 1
Device(config-std-nacl)#permit 225.1.1.0 0.0.0.255
Device(config-std-nacl)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ip igmp access-group 1
Device(config-if-vlan3)#exit
```

Step 4:   Check the result.

#Receiver sends an IGMPv2 membership report to join in the multicast groups 225.1.1.1 and 226.1.1.1.

#Source sends multicast message of multicast groups 225.1.1.1 and 226.1.1.1.

#Check Device's multicast member list.

```
Device#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface             Uptime   Expires  Last Reporter   V1 Expires  V2 Expires
225.1.1.1       vlan3          03:14:59 00:03:05 3.0.0.2          stopped
```

#Check Device's multicast routing table .

```
Device#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:00:56
RP: 0.0.0.0
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    vlan3
  Joined interface list:
  Asserted interface list:


(192.168.1.1, 225.1.1.1)
Up time: 00:00:15
```

```
KAT time: 00:03:15
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
  COULD REGISTER
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    register_vif0
  Asserted interface list:
  Outgoing interface list:
    register_vif0
    vlan3
  Packet count 1

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:00:15
RP: 0.0.0.0
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    vlan3

(192.168.1.1, 226.1.1.1)
Up time: 00:00:15
KAT time: 00:03:15
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
  COULD REGISTER
Upstream State: JOINED
  Local interface list:
```

```
 Joined interface list:
   register_vif0
 Asserted interface list:
 Outgoing interface list:
   register_vif0
 Packet count 1

(192.168.1.1, 226.1.1.1, rpt)
Up time: 00:00:15
RP: 0.0.0.0
Flags:
 RPF SGRPT XG EQUAL
Upstream State: RPT NOT JOINED
 Local interface list:
 Pruned interface list:
 Outgoing interface list:
```

#Receiver can only receive the multicast business message of multicast group 225.1.1.1 sent by Source.

NOTE

- If you want to perform multicast source group based filtering, you can use command ip igmp ssm-access-group to implement the filtering. When the command is used, it is required that the Device runs PIM-SSM and the interface runs IGMPv3.

52 PIM-SM

52.1 PIM-SM Overview

PIM-SM (Protocol Independent Multicast-Sparse Mode) is mainly suitable for circumstances in which group members are distributed sparsely in a wide range or the network bandwidth resources are limited.

PIM-SM is not dependent on any specific unicast routing protocol. The device actively sends join messages to request for establishing multicast distribution tree, and set up RP (Rendezvous Point) and BSR (Bootstrap Router) for advertising multicast information to all PIM-SM routers. When receiver joins in a multicast group, receiving DR (Designated Router) sends PIM join messages to RP, construct a shared tree, the RPT, that has RP as its root. The source DR registers multicast source on RP, constructing a source tree that has multicast source as its root. Multicast business messages are sent along th source tree and shared tree down to the receiver, the receiving DR will send PIM join messages to multicast source and, in the end, switches from RPT to source based SPT (Shortest-path Tree), in order to reduce network delay.

PIM-SSM is the abbreviation of Protocol Independent Multicast-Source Specific Multicast. PIM-SSM is a subset of PIM-SM protocol, it has to run on the basis of PIM-SM. It is stipulated in PIM-SSM protocol that IPv4 addresses 232.0.0.0~232.255.255.255 are reserved for SSM. PIM-SSM has to be used in conjunction with IGMPv3, because IGMPv3 can send IGMP membership report to designated source and group.

52.2 Configuration of PIM-SM Functions

Table 52–1 Functional Configuration List of PIM-SM

Configuration task	
Configure PIM-SM basic functions	Enable PIM-SM protocol
Configure PIM-SM rendezvous point (RP)	Configure C-RP
	Configure static RP
Configure PIM-SM bootstrap router	Configure C-BSR
	Configure BSR border
	Configure RP reachability test

Configuration task	
Configure PIM-SM multicast source registration	Configure register message send rate
	Configure register-stop message send rate
	Configure register message source address
	Configure register message filter
Configure PIM-SM neighbor parameter	Configure Hello message transmission cycle
	Configure neighbor’s Keepalive time
	Configure neighbor filter
	Configure DR priority level
Configure PIM-SM SPT switchover	Configure SPT switchover condition
Configure PIM-SSM	Configure PIM-SSM
Configure PIM-SDM	Enable PIM-SDM

NOTE

- L3 ethernet interface does not support PIM-SM function.

52.2.1 Configure PIM-SM Basic Functions *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of PIM-SM:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Configure any unicast routing protocol to implement intra-domain routing reachability.

Enable PIM-SM Protocol

Table 52–2 Enable PIM-SM Protocol

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable IP multicast forwarding	**ip multicast-routing**	Required By default, IP multicast forwarding is not enabled
Enter the interface configuration mode	**interface** *interface-name*	-
Enable PIM-SM protocol	**ip pim sparse-mode**	To be selected alternatively By default, the interface is in PIM-SM-Off status
	ip pim sparse-mode passive	

NOTE

- After PIM-SM protocol has been enabled, IGMP protocol will be automatically enabled.
- Only after PIM-SM function has been enabled will all PIM-SM related configurations take effect.

52.2.2 Configure PIM-SM Rendezvous Point (RP) *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of RP:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Configure any unicast routing protocol to implement intra-domain routing reachability;
- Enable PIM-SM protocol.

Configure C-RP

RP is generated by C-RP election. Generated by BSR election, all C-RP (Candidate-Rendezvous Point) periodically unicast C-RP messages to BSR, BSR integrates the C-RP information and circulates the information to all devices in PIM-SM domain via bootstrap messages.

Table 52–3 Configure C-RP

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure C-RP	**ip pim rp-candidate** *interface-name* [[*priority-value* [*interval-value* [**group-list** { *access-list-number* | *access-list-name* }]]] | [**group-list** { *access-list-number* | *access-list-name* }]] [**vrf** *vrf-name*]	Required By default, no C-RP

NOTE

● RP selection rules:

1. Perform mask longest match on C-RP service's group range;
2. If mask longest match identifies multiple C-RP, then the priority level of C-RP should be compared. The smaller the value, the higher the priority level. C-RP of higher priority level wins;
3. If more than one C-RP have highest priority level, then HASH value should be calculated for C-RP addresses and group, the C-RP that has the highest HASH value wins;
4. If there are more than one RPs with maximum HASH value, then the C-RP that has the largest IP address wins out.

Configure Static RP

Static RP is recommended for simple PIM-SM networks. Static RP needs no BSR configuration and eliminates frequent interactions between RP and BSR, thereby saving network bandwidth.

Table 52–4 Configure Static RP

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure static RP	**ip pim rp-addressess** *ip-address* [*access-list-name* | *access-list-number*] [**override**] [**vrf** *vrf-name*]	Required By default, no static RP

NOTE

- All devices in the same PIM-SM domain shall be configured the same static RP in order to operate properly.

52.2.3 Configure PIM-SM Bootstrap Router *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of BSR:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Configure any unicast routing protocol to implement intra-domain routing reachability;
- Enable PIM-SM protocol.

Configure C-BSR

In a PIM-SM domain, there must be one and only one BSR. The only recognized BSR is generated by Multiple C-BSR (Candidate-Bootstrap Router)through bootstrap message election.

Table 52–5 Configure C-BSR

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure C-BSR	**ip pim bsr-candidate** *interface_name* [*hash-mask-length* [*priority-value*]] [**vrf** *vrf-name*]	Required By default, no C-BSR

NOTE

- BSR selection rules:

1. Priority levels are compared, the greater the value, the higher the priority level. The one that has the highest priority level wins;
2. If the candidates have identical priority level, then candidate with the greatest IP address wins out.

Configure BSR Border

BSR is responsible for collecting C-RP information and circulating the information to all devices in the PIM-SM domain via bootstrap messages. BSR range is the range of the multicast domain. Bootstrap messages cannot pass through interfaces that have been configured BSR border. Therefore, devices outside the multicast domain range cannot participate in the forwarding of multicast business messages in the multicast domain. Thus, multicast domains are divided.

Table 52–6 Configure BSR Border

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure BSR border	**ip pim bsr-border**	Required By default, there is no multicast border

52.2.4 Configure PIM-SM Multicast Source Registration *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of multicast source register:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Configure any unicast routing protocol to implement intra-domain routing reachability;
- Enable PIM-SM protocol.

Configure RP Reachability Test

Before sending register message to RP, source DR can perform reachability check first. If it is found RP routing is unreachable, source DR will not register with the RP, thereby reducing its expense.

Table 52–7 Configure RP Reachability Test

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure RP reachability test	**ip pim register-rp-reachability** [**vrf** *vrf-name*]	Required By default, RP reachability is not tested before the registration process of PIM.

NOTE

- In order to reduce source DR's expense, it is recommended that all PIM-SM's source DRs are configured the command.

Configure Register Message send Rate

Upon receiving multicast datagram, source DR will encapsulate multicast datagram in register message and send the register message to RP for source register until the register is completed.

When source DR has not completed multicast source register and the multicast traffic is large, a lot of register messages will be generated, increasing the RP device's burden and even giving rise to malfunction of RP. It is not necessary for source DR to send all register messages in the same flow to RP, therefore, source DR is configured a register message send rate that meets the purpose of source register and reduces RP's burden.

Table 52–8 Configure Register Message Send Rate

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure register message send rate	**ip pim register-rate-limit** *rate-limit-value* [**vrf** *vrf-name*]	Required By default, register message send rate is not limited

NOTE

- In order to reduce RP's burden, it is recommended that all source DRs are configured a source register send rate.

Configure Register-Stop Message Send Rate

Upon receiving source DR's register message, RP will send register-stop message to source DR to complete the register process. When receiving numerous register messages, RP needs to reply all register messages (i.e.e, sending register-stop message). In actual scenarios, these register-stop messages contain a lot of duplicate messages. You can reduce RP expenses by limiting the send rate of register-stop messages on RP.

Table 52–9 Configure Register-Stop Message Send Rate

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure send rate of register-stop message	**ip pim register-stop-rate-limit** *rate-limit-value* [**vrf** *vrf-name*]	Required By default, the send rate of register-stop messages is not limited

NOTE

- In order to improve the entire PIM-SM network's robustness, it is recommended to limit the source register stop message rate on all RPs.

Configure Register Message Source Address

When performing source register, source DR will use the register interface's IP address automatically generated by the system as the source address of the register message. The command can specify the register message's source address as the IP address of an interface on the Device to meet certain special requirements of the network.

Table 52–10 Configure Register Message Source Address

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure register message source address	**ip pim register-source interface** *interface-name* [**vrf** *vrf-name*]	Required By default, the IP address of the register interface automatically generated by the system is used for the source address of the register message.

Configure Register Message Filter

In order to prevent source register attack, ACL can be used on RP to perform multicast source filtering of register messages and only ACL permitted multicast sources can be successfully registered on RP.

Table 52–11 Configure Register Message Filter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure register message filter	**ip pim accept-register list** { *access-list-number* | *acees-list-name* } [**vrf** *vrf-name*]	Required By default, register message is not filtered

52.2.5 Configure PIM-SM Neighbor Parameter *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of PIM-SM neighbor parameters:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Configure any unicast routing protocol to implement intra-domain routing reachability;
- Enable PIM-SM protocol.

Configure Hello Message Transmission Cycle

Interfaces that have PIM protocol enabled will periodically send Hello messages to establish and maintain PIM neighbor.

Table 52–12 Configure Hello Message Transmission Cycle

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure Hello message transmission cycle	**ip pim hello-interval** *interval-value*	Optional By default, the transmission cycle of Hello message is 30 seconds

Configure Neighbor's Keepalive Time

When receiving a neighbor's Hello message, the interface will record the holdtime carried in the Hello message as the neighbor's Keepalive time. If no Hello message is received from the neighbor within the Keepalive time, the neighbor is deemed expired.

Table 52–13 Configure PIM-SM Neighbor Keepalive Time

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure neighbor's Keepalive time	**ip pim hello-holdtime** *holdtime-value*	Optional By default, PIM-SM neighbor's Keepalive time is 105 seconds

Configure Neighbor Filter

If there are extraordinarily numerous PIM neighbors in a subnet, you can use neighbor filter function to selectively establish neighbors in order to save device's resources.

Table 52–14 Configure Neighbor Filter

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure neighbor filter	**ip pim neighbor-filter** { *access-list-number* | *acees-list-name* }	Required By default, neighbor filter function is not enabled

Configure DR Priority Level

DR plays a very important role in PIM-SM network. Therefore, the selection of appropriate DR is very critical. You can choose appropriate device as DR by configuring DR priority level.

Only one DR is allowed in a PIM-SM subnet. DRs can be divided into source DRs and receiving DRs by their functions.

The major function of source DR is to perform source register on RP.

The main function of receiving DR is to add to RP and create RPT to SPT switchover.

Table 52–15 Configure DR Priority Level

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure DR priority level	**ip pim dr-priority** *priority-value*	Optional By default, DR priority level is 1

NOTE

- DR selection rules:

1. Priority levels are compared, the greater the value, the higher the priority level. The one that has the highest priority level wins;
2. If the candidates have identical priority level, then candidate with the greatest IP address wins out.

52.2.6 Configure PIM-SM SPT Switchover *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of SPT:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Configure any unicast routing protocol to implement intra-domain routing reachability;
- Enable PIM-SM protocol.

Configure SPT Switchover Condition

Receiving DR does not know the address of multicast source, therefore it has to add to RP to form RPT. Source DR will perform source register with RP, forming a source tree between source DR and RP. In the beginning, the direction of multicast flow is from multicast source to RP, then from RP to receiver. When receiving the first multicast datagram, receiving DR will add to multicast source to form SPT and will prune RPT, this process is what we refer to as SPT switchover.

The function of this command is to configure the conditions for SPT switchover on receiving DR.

Table 52–16 Configure SPT Switchover Condition

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure SPT switchover condition	**ip pim spt-threshold infinity** [**group-list** { *access-list-number* | *acees-list-name* }] [**vrf** *vrf-name*]	Required By default, all multicast groups are capable of SPT switchover

NOTE

- Please do not configure SPT never switch on RP, otherwise, multicast forwarding may fail.

52.2.7 Configure PIM-SSM *-E -A*

PIM-SSM is a subset of PIM-SM. In PIM-SSM, RP and BSR are not required, also not required is RPT. There is no SPT switchover, instead, receiving DR directly add to multicast source and create a source-rooted shortest path tree(SPT).

Configuration Conditions

The following tasks have to be completed prior to the configuration of PIM-SSM:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Configure any unicast routing protocol to implement intra-domain routing reachability;
- Enable PIM-SM protocol on all interfaces for multicast routing forward.

Configure PIM-SSM

Table 52–17 Configure PIM-SSM

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure PIM-SSM	**ip pim ssm** { **default** | **range** { *access-list-number* | *acees-list-name* } } [**vrf** *vrf-name*]	Required By default, SSM function is not turned on

NOTE

- When using PIM-SSM, receiver end DR must have IGMPv3 enabled;
- In case receiver is unable to upgrade to IGMPv3, you can use IGMP SSM Mapping function in conjunction with PIM-SSM;
- It should be ensured that the SSM multicast group address ranges configured on all devices should be consistent, otherwise PIM-SSM may malfunction.

52.2.8 Configure PIM-SM Control Strategy *-E -A*

Configure Interface to Follow the Change of DR Status

Non-DR turns on L2 multicast forwarding, stop L3 multicast forwarding. DR is not affected.

Table 52–18 Configure DR Priority Level

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure DR priority level	**ip pim drchg-attention**	By default, L3 multicast forwarding

Configure Interface to Inhibit PIM JOIN Message

Configure PIM JOIN message to be inhibited by interface.

Table 52–19 Configure to Inhibit Interface PIM JOIN Message

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure interface to inhibit PIM JOIN message	**ip pim join-suppression**	By default, interface PIM JOIN message will not be inhibited

52.2.9 Configure PIM-SM BFD *-E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of PIM-SM BFD:

- Configure interface's network layer address, make various neighboring node network layer reachable;
- Configure any unicast routing protocol to implement intra-domain routing reachability.

Configure PIM-SM BFD

Table 52–20 Configure PIM-SM BFD

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Enable PIM-SM BFD	**ip pim bfd**	By default, PIM-SM BFD function is not enabled

52.2.10 PIM-SM Monitoring and Maintenance *-E -A*

Table 52–21 PIM-SM Monitoring and Maintenance

Command	Description
clear ip pim bsr rp-set [**vrf** *vrf-name*]	Erase PIM-SM's RP set information
clear ip pim mroute [*group-address* [*source-address*]] [**vrf** *vrf-name*]	Erase PIM-SM's multicast routing information
clear ip pim statistics [**interface** *interface-name* | **vrf** *vrf-name*]	Erase PIM-SM protocol message statistical information
show ip pim bsr-router [**vrf** *vrf-name*]	Display PIM-SM bootstrap router information

Command	Description
show ip pim interface [[*interface-name*] **detail**] [**vrf** *vrf-name*]	Display PIM-SM interface information
show ip pim local-members [*interface-name* | **vrf** *vrf-name*]	Display PIM-SM local group member information
show ip pim mroute [**ssm** | **group** *group-ip-address* [**source** *source-ip-address*] | **source** *source-ip-address*] [**vrf** *vrf-name*]	Display PIM-SM multicast routing table information
show ip pim neighbor [**detail**] [**vrf** *vrf-name*]	Display PIM-SM neighboring information
show ip pim nexthop [*ip-address*] [**vrf** *vrf-name*]	Display PIM-SM next router information
show ip pim rp mapping [**vrf** *vrf-name*]	Display PIM-SM's RP information
show ip pim rp-hash *group-address* [**vrf** *vrf-name*]	Display multicast group mapping RP information
show ip pim statistics [**vrf** *vrf-name*]	Display PIM-SM protocol message statistical information

52.3 Example of PIM-SM Typical Configuration

52.3.1 Configure PIM-SM Basic Functions *-E -A*

Network Requirements

- The entire network runs PIM-SM protocol.
- Receiver1, Receiver2 are two receivers of Device3 stub network.
- Device1, Device2 are C-BSR and C-RP.
- IGMPv2 runs between Device3 and stub network.

Network Topology

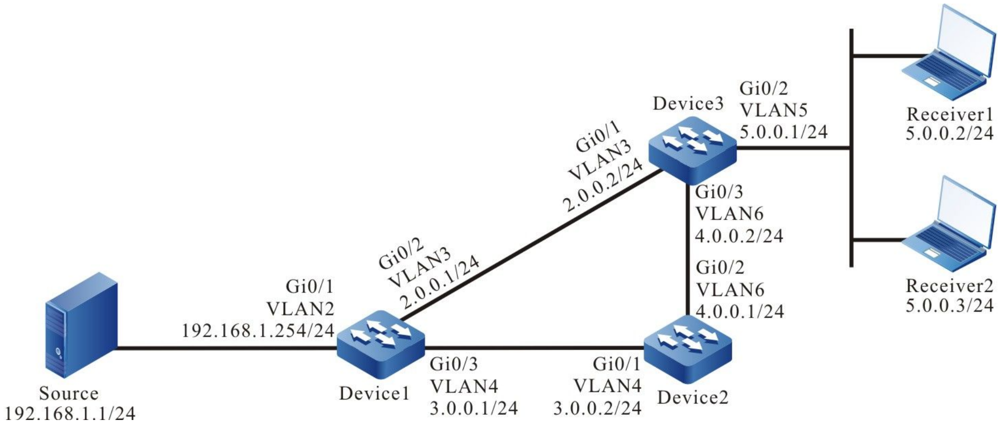


Figure 52-1 Networking Diagram - Configure PIM-SM Basic Functions

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Turn on unicast routing protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 14:48:47, vlan3
O   3.0.0.0/24 [110/2] via 2.0.0.1, 14:31:14, vlan3
               [110/2] via 4.0.0.1, 14:31:04, vlan6
C   4.0.0.0/24 is directly connected, 15:36:57, vlan6
C   5.0.0.0/24 is directly connected, 14:09:18, vlan5
O   192.168.1.0/24 [110/2] via 2.0.0.1, 00:30:55, vlan3
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 3: Globally enable multicast forwarding, enable multicast protocol PIM-SM on interfaces.

#Configure Device1.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ip pim sparse-mode
```

```
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan6
Device2(config-if-vlan6)#ip pim sparse-mode
Device2(config-if-vlan6)#exit
```

#Configure Device3.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ip pim sparse-mode
Device3(config-if-vlan6)#exit
```

#Check information on interfaces that have been enabled PIM-SM protocol on Device3 and PIM-SM neighboring information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address      Interface           VIF    Ver/   VIF   Nbr    DR    DR         BSR    CISCO    Neighbor
                              Index   Mode   Flag  Count  Pri              Border Neighbor Filter
2.0.0.2      vlan3      0     v2/S   UP    1     1     2.0.0.2      FALSE  FALSE
5.0.0.1      vlan5      2     v2/S   UP    0     1     5.0.0.1      FALSE  FALSE
4.0.0.2      vlan6      3     v2/S   UP    1     1     4.0.0.2      FALSE  FALSE

Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 2 Neighbor entries
Neighbor      Interface           Uptime/Expires    Ver   DR
Address                                          Priority/Mode
2.0.0.1       vlan3     01:12:00/00:01:39 v2    1 /
```

```
4.0.0.1          vlan6      01:13:19/00:01:35 v2    1 /
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

#Check interface vlan5's IGMP information on Device3.

```
Device3#show ip igmp interface vlan5
Interface vlan5 (Index 50332250)
 IGMP Active, Querier (5.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 5.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

NOTE

- The configuration of multicast protocol on interface automatically enables IGMP function; by default, IGMPv2 will run. Use command ip igmp version can configure the version of IGMP running on the interface.

Step 4: Configure Device1's interface vlan3 as C-BSR and C-RP, configure Device2's interface vlan4 as C-BSR and C-RP.

#Configure Device1.

Configure Device1's interface vlan3 as C-BSR and C-RP, C-BSR's priority level to 200, C-RP service’s multicast group range to 230.0.0.0/8.

```
Device1(config)#ip pim bsr-candidate vlan 3 10 200
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 230.0.0.0 0.255.255.255
Device1(config-std-nacl)#exit
Device1(config)#ip pim rp-candidate vlan 3 group-list 1
```

#Configure Device2.

Configure Device2's vlan4 as C-BSR and C-RP, C-BSR's priority level to 0, Device2's C-RP service’s multicast group range to 224.0.0.0/4.

```
Device2(config)#ip pim bsr-candidate vlan4
Device2(config)#ip pim rp-candidate vlan4
```

#Check Device3's BSR and RP information

```
Device3#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 2.0.0.1
  BSR Priority: 200
  Hash mask length: 10
  Up time: 01:03:30
  Expiry time: 00:01:46
  Role: Non-candidate BSR
  State: Accept Preferred

Device3#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 2 RP set entries
Total 2 RP entries

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 3.0.0.2
      Info source: 2.0.0.1, via bootstrap, priority 192
      Up time: 01:03:29
      Expiry time: 00:02:02

  Group(s): 230.0.0.0/8
  RP count: 1
    RP: 2.0.0.1
      Info source: 2.0.0.1, via bootstrap, priority 192
      Up time: 01:15:50
      Expiry time: 00:02:02
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.
- When a multicast domain is configured multiple C-BSRs, BSR will be elected according to the priority level of C-BSR. The C-BSR that has the highest priority level will be elected as BSR. When C-BSRs are of the same priority level, the C-BSR that has the largest ip address will be elected as BSR;
- When a multicast domain is configured multiple C-RPs that serve the same multicast group range, the RP corresponding to the multicast group G will be calculated with hash algorithm;
- In multicast domain, RP can also be configured with the command ip pim rp-address, but it is required that the static RP addresses configured on all devices in the entire multicast domain shall remain consistent.

Step 5: Check the result.

#Receiver1 and Receiver2 send an IGMPv2 membership report to join in the multicast groups 225.1.1.1,230.1.1.1.

#Source sends multicast business messages of multicast group 225.1.1.1,230.1.1.1.

#Check multicast member list on Device3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 2 groups
Group Address   Interface        Uptime   Expires  Last Reporter   V1 Expires  V2 Expires
225.1.1.1       vlan5            00:56:48 00:02:39 5.0.0.2         stopped
230.1.1.1       vlan5            00:56:48 00:02:46 5.0.0.3         stopped
```

#Check the RP corresponding to multicast groups 225.1.1.1,230.1.1.1, respectively, on Device3.

```
Device3#show ip pim rp-hash 225.1.1.1
 PIM VRF Name: Default
 RP: 3.0.0.2
  Info source: 2.0.0.1, via bootstrap

Device3#show ip pim rp-hash 230.1.1.1
 PIM VRF Name: Default
 RP: 2.0.0.1
  Info source: 2.0.0.1, via bootstrap
```

#Check multicast routing table of Device3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
```

```
Total 0 (*,*,RP) entry
Total 2 (*,G) entries
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer

(*, 225.1.1.1)
Up time: 00:36:21
RP: 3.0.0.2
RPF nbr: 4.0.0.1
RPF idx: vlan6
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    vlan5
  Joined interface list:
  Asserted interface list:

(192.168.1.1, 225.1.1.1)
Up time: 00:36:02
KAT time: 00:03:11
RPF nbr: 4.0.0.1
RPF idx: vlan6
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    vlan5
  Packet count 2517423

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:36:02
RP: 3.0.0.2
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    vlan5

(*, 230.1.1.1)
Up time: 00:36:21
RP: 2.0.0.1
RPF nbr: 2.0.0.1
RPF idx: vlan3
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    vlan5
  Joined interface list:
  Asserted interface list:

(192.168.1.1, 230.1.1.1)
Up time: 00:36:02
KAT time: 00:03:11
RPF nbr: 2.0.0.1
RPF idx: vlan3
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    vlan5
  Packet count 2517712

(192.168.1.1, 230.1.1.1, rpt)
Up time: 00:36:02
```

```
RP: 2.0.0.1
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
```

#Receiver1 can only receive the multicast business message of multicast group 225.1.1.1 sent by Source. Receiver2 can only receive the multicast business message of multicast group 230.1.1.1 sent by Source.

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.
- By default, the Device has SPT switchover enabled.

52.3.2 Configure PIM-SSM *-E -A*

Network Requirements

- The entire network runs PIM-SSM protocol.
- Receiver: a receiver in Device3 stub network.
- IGMPv3 runs between Device3 and stub network.

Network Topology

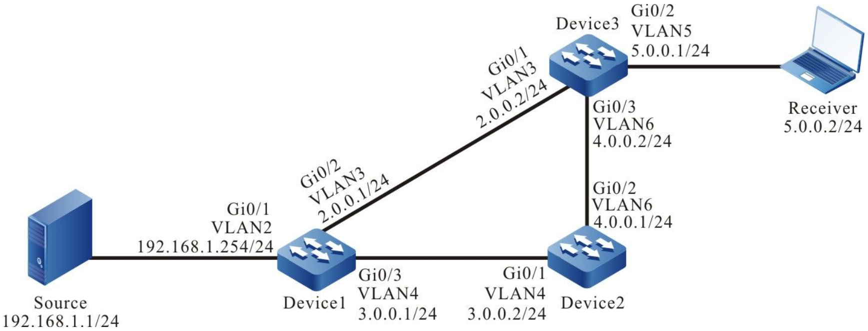


Figure 52-2 Networking Diagram - Configure PIM-SSM

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Turn on unicast routing protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 14:48:47, vlan3
O   3.0.0.0/24 [110/2] via 2.0.0.1, 14:31:14, vlan3
         [110/2] via 4.0.0.1, 14:31:04, vlan6
C   4.0.0.0/24 is directly connected, 15:36:57, vlan6
C   5.0.0.0/24 is directly connected, 14:09:18, vlan5
O   192.168.1.0/24 [110/2] via 2.0.0.1, 00:30:55, vlan3
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 3: Globally enable multicast forwarding, enable multicast protocol PIM-SM on interfaces.

#Configure Device1.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan6
Device2(config-if-vlan6)#ip pim sparse-mode
Device2(config-if-vlan6)#exit
```

#Configure Device3.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
```

```
Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ip pim sparse-mode
Device3(config-if-vlan6)#exit
```

#Check information on interfaces that have been enabled PIM-SM protocol on Device3 and PIM-SM neighboring information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address       Interface            VIF    Ver/   VIF   Nbr    DR    DR         BSR    CISCO    Neighbor
                             Index    Mode   Flag  Count  Pri            Border Neighbor Filter
2.0.0.2       vlan3        3       v2/S   UP    1      1     2.0.0.2       FALSE  FALSE
5.0.0.1       vlan5        0       v2/S   UP    0      1     5.0.0.1       FALSE  FALSE
4.0.0.2       vlan6        2       v2/S   UP    1      1     4.0.0.2       FALSE  FALSE

Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 2 Neighbor entries
Neighbor       Interface              Uptime/Expires    Ver   DR
Address                                          Priority/Mode
2.0.0.1        vlan3                01:12:00/00:01:39 v2    1 /
4.0.0.1        vlan6                01:13:19/00:01:35 v2    1 /
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 4: Configure PIM-SSM on all devices, SSM service’s multicast group range is 232.0.0.0/8. Device3's vlan5 runs IGMPv3.

#Configure Device1.

```
Device1(config)#ip pim ssm default
```

#Configure Device2.

```
Device2(config)#ip pim ssm default
```

#Configure Device3.

```
Device3(config)#ip pim ssm default
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ip igmp version 3
Device3(config-if-vlan5)#exit
```

#Check interface vlan5's IGMP information on Device3.

```
Device3#show ip igmp interface vlan5
Interface vlan5 (Index 50332250)
 IGMP Enabled, Active, Querier (5.0.0.1)
 Configured for version 3
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 5.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

Step 5: Check the result.

#Receiver sends an IGMPv3 membership report of designated source group to join in the multicast group 232.1.1.1, the designated multicast source is 192.168.1.1.

#Source sends multicast business messages of multicast group 232.1.1.1.

#Check multicast member list of Device3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address    Interface          Uptime   Expires  Last Reporter   V1 Expires  V2 Expires
232.1.1.1        vlan5           00:11:14  stopped 5.0.0.2          stopped    stopped

Device3#show ip igmp groups detail
Interface:      vlan5
Group:          232.1.1.1
Uptime:          00:11:20
Group mode:     Include
```

```
Last reporter:  5.0.0.2
TIB-A Count:    1
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
  192.168.1.1     00:11:20  00:03:28  stopped   Yes  R
```

#Check multicast routing table of Device3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entry
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer

(192.168.1.1, 232.1.1.1)
Up time: 12:59:27
KAT time: 00:03:20
RPF nbr: 2.0.0.1
RPF idx: vlan3
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
   vlan5
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    vlan5
  Packet count 109783214
```

#Receiver can only receive the multicast business message of multicast group 232.1.1.1 sent by Source.

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.
- PIM-SSM's default multicast group range is 232.0.0.0/8, use command ip pim ssm range can change the PIM-SSM service’s multicast group range.
- For multicast group G meeting the SSM conditions, the multicast routing table will not generate (*,G) table entry, instead, it will only generate (S,G)table entry.

52.3.3 Configure PIM-SM Multicast Forwarding Control *-E -A*

Network Requirements

- The entire network runs PIM-SM protocol.
- Receiver: a receiver in Device3 stub network.
- Device2 is C-BSR and C-RP.
- On Device2 and Device3, control the multicast sources so that Receiver can only receive multicast business messages sent by Source1.
- IGMPv2 runs between Device3 and stub network.

Network Topology

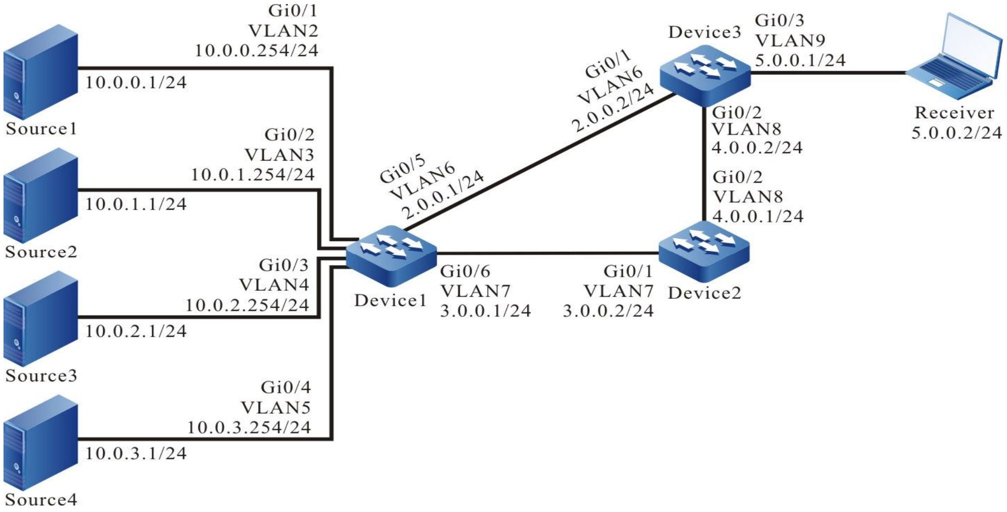


Figure 52-3 Networking Diagram - Configure PIM-SM Multicast Forwarding Control

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Turn on unicast routing protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal

Device1(config)#router ospf 100
```

```
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.0 0.0.255.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 15:51:07, vlan6
O   3.0.0.0/24 [110/2] via 2.0.0.1, 15:33:34, vlan6
             [110/2] via 4.0.0.1, 15:33:24, vlan8
C   4.0.0.0/24 is directly connected, 16:39:17, vlan8
C   5.0.0.0/24 is directly connected, 15:11:38, vlan9
O   10.0.0.0/24 [110/2] via 2.0.0.1, 00:06:32, vlan6
O   10.0.1.0/24 [110/2] via 2.0.0.1, 00:06:32, vlan6
O   10.0.2.0/24 [110/2] via 2.0.0.1, 00:06:32, vlan6
O   10.0.3.0/24 [110/2] via 2.0.0.1, 00:06:32, vlan6
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 3: Globally enable multicast forwarding, enable multicast protocol PIM-SM on interfaces.

#Configure Device1.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ip pim sparse-mode
Device1(config-if-vlan5)#exit
Device1(config)#interface vlan6
Device1(config-if-vlan6)#ip pim sparse-mode
Device1(config-if-vlan6)#exit
Device1(config)#interface vlan7
Device1(config-if-vlan7)#ip pim sparse-mode
Device1(config-if-vlan7)#exit
```

#Configure Device2.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan7
Device2(config-if-vlan7)#ip pim sparse-mode
Device2(config-if-vlan7)#exit
Device2(config)#interface vlan8
Device2(config-if-vlan8)#ip pim sparse-mode
Device2(config-if-vlan8)#exit
```

#Configure Device3.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ip pim sparse-mode
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
Device3(config-if-vlan8)#ip pim sparse-mode
Device3(config-if-vlan8)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ip pim sparse-mode
Device3(config-if-vlan9)#exit
```

#Check information on interfaces that have been enabled PIM-SM protocol on Device3 and PIM-SM neighboring information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address       Interface          VIF     Ver/   VIF   Nbr    DR        DR          BSR    CISCO    Neighbor
                             Index    Mode   Flag  Count  Priority              Border Neighbor Filter
2.0.0.2        vlan6    2      v2/S   UP    1      1        2.0.0.2       FALSE  FALSE
4.0.0.2        vlan8    0      v2/S   UP    1      1        4.0.0.2       FALSE  FALSE
5.0.0.1       vlan9     3      v2/S   UP    0      1        5.0.0.1       FALSE  FALSE

Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 2 Neighbor entries

Neighbor        Interface            Uptime/Expires    Ver   DR
Address                                          Priority/Mode
2.0.0.1         vlan6               00:50:29/00:01:19 v2    1 /
4.0.0.1         vlan8               00:57:58/00:01:33 v2    1 /
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 4: Configure Device2's vlan7 as the entire network's C-BSR and C-RP, and configure C-RP service’s multicast group range to 224.0.0.0/4.

#Configure Device2.

```
Device2(config)#ip pim bsr-candidate vlan7
Device2(config)#ip pim rp-candidate vlan7
```

#Check Device3's BSR and RP information.

```
Device3#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 3.0.0.2
  BSR Priority: 0
  Hash mask length: 10
  Up time: 00:10:37
  Expiry time: 00:01:33
  Role: Non-candidate BSR
  State: Accept Preferred

Device3#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 3.0.0.2
      Info source: 3.0.0.2, via bootstrap, priority 192
      Up time: 03:59:59
      Expiry time: 00:01:49
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 5: On Device2/Device3, control the multicast sources so that Receiver can only receive multicast business messages sent by Source1.

#On Device2, configure the acceptable register message access list, filter out Source4's register message.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#deny 10.0.3.0 0.0.0.255
Device2(config-std-nacl)#permit any
Device2(config-std-nacl)#exit
Device2(config)#ip pim accept-register list 1
```

#On Device3's interface vlan6/vlan8, configure acl of incoming direction, filter out Source3';s multicast business message.

```
Device3(config)#ip access-list extended 1001
Device3(config-ext-nacl)#deny ip 10.0.2.0 0.0.0.255 224.0.0.0 31.255.255.255
Device3(config-ext-nacl)#permit igmp any any
Device3(config-ext-nacl)#permit pim any any
Device3(config-ext-nacl)#permit ospf any any
Device3(config-ext-nacl)#permit ip any any
Device3(config-ext-nacl)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ip access-group 1001 in
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
Device3(config-if-vlan8)#ip access-group 1001 in
Device3(config-if-vlan8)#exit
```

#On Device3's interface vlan9,configure acl of outgoing direction, filter out Source2's multicast business message.

```
Device3(config)#ip access-list extended 1002
Device3(config-ext-nacl)#deny ip 10.0.1.0 0.0.0.255 224.0.0.0 31.255.255.255
Device3(config-ext-nacl)#permit igmp any any
Device3(config-ext-nacl)#permit pim any any
Device3(config-ext-nacl)#permit ip any any
Device3(config-ext-nacl)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ip access-group 1002 out
Device3(config-if-vlan9)#exit
```

Step 6: Check the result.

#Receiver sends an IGMPv2 membership report to join in the multicast group 225.1.1.1.

#Source1, Source2, Source3, and Source4 all send multicast business message to multicast group 225.1.1.1.

#Check Device2's multicast member list.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address    Interface          Uptime   Expires  Last Reporter   V1 Expires  V2 Expires
225.1.1.1        vlan9              00:00:38 00:03:45 5.0.0.2         stopped
```

#Check multicast routing table of Device3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:07:55
RP: 3.0.0.2
RPF nbr: 4.0.0.1
RPF idx: vlan8
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    vlan9
  Joined interface list:
  Asserted interface list:


(10.0.0.1, 225.1.1.1)
Up time: 00:07:49
KAT time: 00:03:17
```

```
RPF nbr: 2.0.0.1
RPF idx: vlan6
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    vlan9
  Packet count 268411

(10.0.0.1, 225.1.1.1, rpt)
Up time: 00:07:49
RP: 3.0.0.2
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    vlan9

(10.0.1.1, 225.1.1.1)
Up time: 00:07:49
KAT time: 00:03:17
RPF nbr: 2.0.0.1
RPF idx: vlan6
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
   vlan9
  Packet count 268237

(10.0.1.1, 225.1.1.1, rpt)
Up time: 00:07:49
RP: 3.0.0.2
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
vlan9
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

#Check Device2's acl matching.

```
Device2#show ip access-list 1
ip access-list standard 1
 10 deny 10.0.3.0 0.0.0.255     32 matches
 20 permit any     2767 matches
```

#Check Device3's acl matching.

```
Device3#show ip access-list  1001
ip access-list extended 1001
 10 deny ip 10.0.2.0 0.0.0.255 224.0.0.0 31.255.255.255     671545 matches
 20 permit igmp any any     19 matches
 30 permit pim any any     119 matches
 40 permit ospf any any     252 matches
 50 permit ip any any     1343339 matches

Device3#show ip access-list  1002
ip access-list extended 1002
 10 deny ip 10.0.1.0 0.0.0.255 224.0.0.0 31.255.255.255     672358 matches
 20 permit igmp any any     10 matches
 30 permit pim any any     40 matches
```

```
40 permit ip any any     672532 matches
```

#Receive can only receive multicast business messages sent by Source1.

NOTE

- When performing multicast source control, it is preferred to configure multicast source control first and then the on-demand multicast source. This is because, by default, receiving DR only performs SPT switchover upon the receipt of multicast business message. If multicast source is on demand first prior to multicast forwarding control, then multicast forwarding control will not work. In order to prevent the malfunction of multicast forwarding control, it is acceptable to disable STP switchover in receiving DR configuration.

52.3.4 Configure DR Switchover Convergence for PIM-SM to Work with BFD *-E -A*

Network Requirements

- The entire network runs PIM-SM protocol.
- Device1 is C-BSR and C-RP.
- Device2 and Device3 are in the stub network where the Receiver is located, Device3 serves the role of receiver DR.
- Enable PIM BFD on the line between Device2 and Device3, when the line between Device3 and Receiver malfunctions, Device2 will fast switchover to receiver DR.

Network Topology

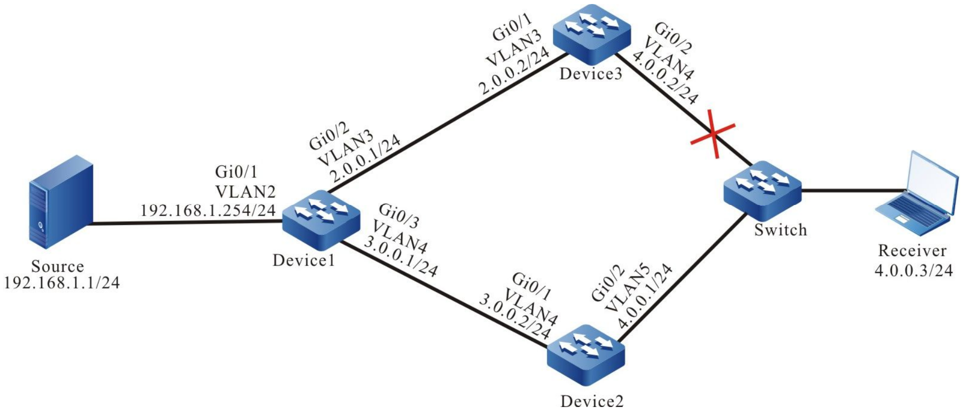


Figure 52-4 Networking Diagram - Configure DR Switching for PIM-SM to Work with BFD

Configuration Steps

Step 1: Configure IP addresses of the interfaces (omitted).

Step 2: Turn on unicast routing protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#Query the routing table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 14:48:47, vlan3
O   3.0.0.0/24 [110/2] via 2.0.0.1, 14:31:14, vlan3
            [110/2] via 4.0.0.1, 14:31:04, vlan4
C   4.0.0.0/24 is directly connected, 15:36:57, vlan4
O   192.168.1.0/24 [110/2] via 2.0.0.1, 00:30:55, vlan3
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 3: Globally enable multicast forwarding, enable multicast protocol PIM-SM on interfaces.

#Configure Device1.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device1(config)#ip multicast-routing
```

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan 5
Device2(config-if-vlan5)#ip pim sparse-mode
Device2(config-if-vlan5)#exit
```

#Configure Device3.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ip pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim sparse-mode
Device3(config-if-vlan4)#exit
```

#Check information on interfaces that have been enabled PIM-SM protocol on Device3 and PIM-SM neighboring information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 2 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address      Interface           VIF    Ver/  VIF  Nbr   DR    DR          BSR   CISCO   Neighbor
                               Index   Mode  Flag  CountPri            Border Neighbor Filter
2.0.0.2      vlan3                 2     v2/S  UP    1    1   2.0.0.2      FALSE  FALSE
4.0.0.2      vlan4                 0     v2/S  UP    1    1   4.0.0.2      FALSE  FALSE
```

```
Device3#show ip pim neighbor

PIM Neighbor Table:

PIM VRF Name: Default

Total 2 Neighbor entries


NeighborInterface      Uptime/Expires    VerDR

Address                               Priority/Mode

4.0.0.1   vlan4       00:11:26/00:01:19   v2    1 /

2.0.0.1   vlan3       00:05:57/00:01:18   v2    1 /
```

#It can be seen that Device3 is the receiver DR in the stub network where the Receiver is located.

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 4: Configure C-BSR and C-RP.

#Configure Device1.

Configure Device1's vlan2 as the entire network's C-BSR and C-RP, and configure C-RP service’s multicast group range to 224.0.0.0/8.

```
Device1(config)#ip pim bsr-candidate vlan 2

Device1(config)#ip pim rp-candidate vlan 2
```

#Check Device3's BSR and RP information.

```
Device3#show ip pim bsr-router

PIMv2 Bootstrap information

PIM VRF Name: Default

   BSR address: 192.168.1.254

  BSR Priority: 0

  Hash mask length: 10

  Up time: 00:00:17

  Expiry time: 00:01:56

  Role: Non-candidate BSR

  State: Accept Preferred


Device3#show ip pim rp mapping

PIM Group-to-RP Mappings Table:

PIM VRF Name: Default
```

```
Total 1 RP set entry
Total 1 RP entry

 Group(s): 224.0.0.0/4
 RP count: 1
  RP: 192.168.1.254
   Info source: 192.168.1.254, via bootstrap, priority 192
   Up time: 00:00:16
   Expiry time: 00:02:14
```

NOTE

- Device1 and Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 5: On Device2, Device3, configure PIM to work with BFD.

#Configure Device2.

```
Device2(config)#interface vlan 5
Device2(config-if-vlan5)#ip pim bfd
Device2(config-if-vlan5)#exit
```

#Configure Device3.

```
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim bfd
Device3(config-if-vlan4)#exit
```

#Check Device3's BFD dialog information.

```
Device3#show bfd session detail
Total session number: 1
OurAddr    NeighAddr          LD/RD            State      Holddown    Interface
4.0.0.2    4.0.0.1            5/1              UP         5000        vlan4
Type:ipv4 direct
Local State:UP  Remote State:UP Up for: 0h:6m:39s  Number of times UP:1
Send Interval:1000ms  Detection time:3000ms(1000ms*3)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:1000  MinRxInt:1000  Multiplier:5
Remote MinTxInt:10  Remote MinRxInt:10  Remote Multiplier:3
Registered protocols:PIM
Agent session info:
Sender:slot 2  Recver:slot 2
```

#It can be seen that PIM is successfully associated with BFD.

NOTE

- Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 6: Check the result.

#Receiver sends an IGMPv2 membership report to join in the multicast group225.1.1.1, Source sends a multicast business message of the multicast group 225.1.1.1.

#Check multicast member list on Device2 and Device3, respectively.

```
Device2#show ip igmp groups

IGMP Connected Group Membership

Total 1 groups

Group Address    Interface                    Uptime   Expires  Last Reporter   V1 Expires  V2 Expires

225.1.1.1        vlan5                   00:00:56 00:03:25 4.0.0.3          stopped


Device3#show ip igmp groups

IGMP Connected Group Membership

Total 1 groups

Group Address    Interface                    Uptime   Expires  Last Reporter   V1 Expires  V2 Expires

225.1.1.1        vlan4                   00:00:02 00:04:17 4.0.0.3          stopped
```

#Check PIM-SM multicast routing table on Device2 and Device3, respectively.

```
Device2#show ip pim mroute

IP Multicast Routing Table:

PIM VRF Name: Default

Total 0 (*,*,RP) entry

Total 1 (*,G) entry

Total 0 (S,G) entry

Total 0 (S,G,rpt) entry

Total 0 FCR entry

Up timer/Expiry timer



(*, 225.1.1.1)

Up time: 00:04:27

RP: 192.168.1.254

RPF nbr: 0.0.0.0

RPF idx: None

Flags:

Upstream State: NOT JOINED
```

```
  Local interface list:
      vlan5
  Joined interface list:
  Asserted interface list:

Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:02:10
RP: 192.168.1.254
RPF nbr: 2.0.0.1
RPF idx: vlan3
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
     vlan4
  Joined interface list:
  Asserted interface list:


(192.168.1.1, 225.1.1.1)
Up time: 00:00:37
KAT time: 00:02:53
RPF nbr: 2.0.0.1
RPF idx: vlan3
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
```

```
  Joined interface list:
  Asserted interface list:
 Outgoing interface list:
          vlan4
  Packet count 0

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:00:37
RP: 192.168.1.254
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list
```

#It can be seen the upstream status of the PIM-SM multicast routing table on Device2 is NOT JOINED, the upstream status of multicast routing on Device3 is JOINED, and multicast business message is forwarded to Receiver via Device3.

#When the line between Device3 and Receiver malfunctions, BFD will fast detect the fault and notify PIM-SM protocol, and Device2 will fast switchover to receiver DR.

#Check Device2's PIM-SM neighboring information, BFD dialog information and PIM-SM multicast routing table.

```
Device2#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

Neighbor      Interface              Uptime/Expires      Ver   DR
Address                                          Priority/Mode
3.0.0.1       vlan4                  01:12:27/00:01:31   v2    1 /

Device2#show bfd session detail
Total session number: 0

Device2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:01:03
RP: 192.168.1.254
RPF nbr: 3.0.0.1
RPF idx: vlan4
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
              vlan5
  Joined interface list:
  Asserted interface list:


(192.168.1.1, 225.1.1.1)
Up time: 00:00:42
KAT time: 00:02:48
RPF nbr: 3.0.0.1
RPF idx: vlan4
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
                vlan5
  Packet count 0

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:00:42
RP: 192.168.1.254
Flags:
  RPT JOIN DESIRED
```

```
 RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
 Local interface list:
 Pruned interface list:
 Outgoing interface list:
```

#Check Device3's PIM-SM neighbors, BFD dialog and multicast routing table.

```
Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

Neighbor        Interface                  Uptime/Expires      Ver   DR
Address                                                   Priority/Mode
2.0.0.1         vlan3                   00:12:27/00:01:20   v2    1 /

Device3#show bfd session detail
Total session number: 0

Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 0(S,G) entry
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

#It can be seen that when receiver DR Device3 fails, BFD dialog will immediately respond, Device2 will switchover to receiver DR, multicast business message will be forwarded to Receiver via Device2.

NOTE

- The cooperation of BFD and PIM also applies to the scenario of Assert election in a shared network segment, when the Assert Winner's interface malfunctions, Assert Loser can fast respond to resume the forwarding of multicast message.

52.3.5 Configure RPF Routing Switchover Convergence for PIM-SM to Work with BFD

-E -A

Network Requirements

- The entire network runs PIM-SM protocol.
- Device2 is C-BSR and C-RP.
- The entire network uses OSPF interactive unicast routing.
- PIM BFD and OSPF BFD detection functions are enabled on the line between Device1 and Device3. When the line malfunctions, BFD may fast detect the fault and notify PIM and OSPF protocol, so that the RPF neighbor from Device3 to multicast source fast switchover to Device2.

Network Topology

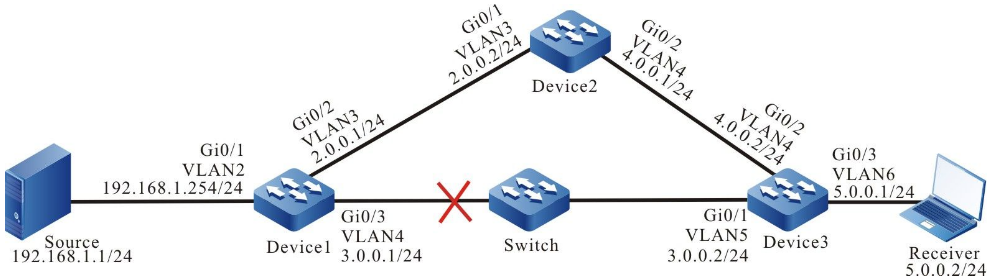


Figure 52-5 Networking Diagram - Configure RPF Routing Switch for PIM-SM to Work with BFD

Configuration steps

Step 1: Configure IP addresses of the interfaces (omitted).

Step 2: Turn on unicast routing protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
```

```
Device3(config-ospf)#exit
```

#Check Device3's unicast routing table.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   3.0.0.0/24 is directly connected, 00:01:40, vlan5
C   4.0.0.0/24 is directly connected, 00:00:46, vlan4
C   5.0.0.0/24 is directly connected, 03:45:18, vlan6
C   127.0.0.0/8 is directly connected, 2d:08:42:01, lo0
O   192.168.1.0/24 [110/2] via 3.0.0.1, 00:01:29, vlan5
O   2.0.0.0/24 [110/2] via 4.0.0.1, 00:01:29, vlan4
           [110/2] via 3.0.0.1, 00:01:29, vlan5
```

NOTE

- Device1, Device2's checking method is similar to that of Device3, the checking process is omitted here.

Step 3: Globally enable multicast forwarding, enable multicast protocol PIM-SM on interfaces.

#Configure Device1.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ip pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ip pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#ip pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip pim sparse-mode
```

```
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ip pim sparse-mode
Device2(config-if-vlan4)#exit
```

#Configure Device3.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on relevant interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim sparse-mode
Device3(config-if-vlan4)#exit
Device3(config)#interface vlan 6
Device3(config-if-vlan6)#ip pim sparse-mode
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan 5
Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
```

#Check information on interfaces that have been enabled PIM-SM protocol on Device3 and PIM-SM neighboring information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address     Interface          VIF    Ver/   VIF  Nbr   DR    DR        BSR   CISCO   Neighbor
                             Index  Mode   Flag  CountPri            Border Neighbor Filter
4.0.0.2     vlan4                 0     v2/S   UP    1     1    4.0.0.2     FALSE  FALSE
5.0.0.1     vlan6                 2     v2/S   UP    0     1    5.0.0.1     FALSE  FALSE
3.0.0.2     vlan5                 3     v2/S   UP    1     1    3.0.0.2     FALSE  FALSE

Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 2 Neighbor entries

Neighbor      Interface            Uptime/Expires     Ver   DR
Address                                               Priority/Mode
4.0.0.1       vlan4              00:05:26/00:01:20   v2    1 /
3.0.0.1       vlan5              00:03:51/00:01:24   v2    1 /
```

Step 4: Configure C-BSR and C-RP.

#Configure Device2.

Configure Device2's vlan3 as the entire network's C-BSR and C-RP, and configure C-RP service's multicast group range to 224.0.0.0/8.

```
Device2(config)#ip pim bsr-candidate vlan 3
Device2(config)#ip pim rp-candidate vlan 3
```

#Check Device3's BSR and RP information.

```
Device3#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
   BSR address: 2.0.0.2
  BSR Priority: 0
  Hash mask length: 10
  Up time: 00:02:56
  Expiry time: 00:01:14
  Role: Non-candidate BSR
  State: Accept Preferred

Device3#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): 224.0.0.0/4
  RP count: 1
      RP: 2.0.0.2
    Info source: 2.0.0.2, via bootstrap, priority 192
    Up time: 00:02:58
    Expiry time: 00:01:32
```

Step 5: On Device1, Device3, configure PIM, OSPF to work with BFD.

#Configure Device1.

```
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#ip pim bfd
Device1(config-if-vlan4)#ip ospf bfd
Device1(config-if-vlan4)#exit
```

#Configure Device3.

```
Device3(config)#interface vlan 5
Device3(config-if-vlan5)#ip pim bfd
```

```
Device3(config-if-vlan5)#ip ospf bfd
Device3(config-if-vlan5)#exit
```

#Check Device3's BFD dialog information.

```
Device3#show bfd session detail
Total session number: 1
OurAddr     NeighAddr           LD/RD               State       Holddown    Interface
3.0.0.2     3.0.0.1                  5/2                   UP          5000        vlan5
Type:ipv4 direct
Local State:UP  Remote State:UP Up for: 0h:2m:35s  Number of times UP:1
Send Interval:1000ms  Detection time:5000ms(1000ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:1000  MinRxInt:1000  Multiplier:5
Remote MinTxInt:1000  Remote MinRxInt:1000  Remote Multiplier:5
Registered protocols:OSPF  PIM
Agent session info:
Sender:slot 1  Recver:slot 1
```

#It can be seen that BFD dialog has been normally established between Device1 and Device3, and has been successfully associated with OSPF and PIM protocol.

NOTE

- Device1's checking method is similar to that of Device3, the checking process is omitted here.

Step 6: Check the result.

#Receiver sends an IGMPv2 membership report to join in the multicast group225.1.1.1, Source sends a multicast business message of the multicast group 225.1.1.1.

#Check multicast member list of Device3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address    Interface                    Uptime   Expires  Last Reporter   V1 Expires  V2 Expires
225.1.1.1        vlan6                    02:55:24 00:04:18 5.0.0.3          stopped
```

#Check Device3's PIM-SM multicast routing table.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 02:57:30
RP: 2.0.0.2
RPF nbr: 4.0.0.1
RPF idx: vlan4
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
             vlan6
  Joined interface list:
  Asserted interface list:


(192.168.1.1, 225.1.1.1)
Up time: 00:12:58
KAT time: 00:03:03
RPF nbr: 3.0.0.1
RPF idx: vlan5
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
             vlan6
  Packet count 620657

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:12:58
RP: 2.0.0.2
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
```

```
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
```

#It can be seen that the RPF neighbor from Device3 to multicast source is Device1, the multicast business message's incoming interface is vlan5.

#When the line between Device1 and Device3 malfunctions, BFD will fast detect the fault and notify OSPF and PIM protocol, OSPF will switch the routing to Device2 for communication, and notify PIM protocol of the unicast routing change, PIM protocol will fast switch to the multicast source's RPF neighbor.

#Check Device3's PIM-SM neighbor and multicast routing table.

```
Apr 27 2016 06:59:26: %BFD-SESSION_DOWN-4: Session [destination address:3.0.0.1,source address:3.0.0.2,interface:vlan5,local-discriminator:4] DOWN

Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

Neighbor      Interface          Uptime/Expires    Ver   DR
Address                                            Priority/Mode
4.0.0.1       vlan4              00:34:40/00:01:37   v2    1 /

Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer



(*, 225.1.1.1)
Up time: 03:07:04
RP: 2.0.0.2
RPF nbr: 4.0.0.1
RPF idx: vlan4
Flags:
  JOIN DESIRED
Upstream State: JOINED
```

```
  Local interface list:
    vlan6
  Joined interface list:
  Asserted interface list:



(192.168.1.1, 225.1.1.1)
Up time: 00:22:32
KAT time: 00:03:29
RPF nbr: 4.0.0.1
RPF idx: vlan4
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
            vlan6
  Packet count 1127697

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:22:32
RP:2.0.0.2
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
            vlan6
```

#It can be seen that the RPF neighbor from Device3 to multicast source is switched to Device2, the multicast business message's incoming interface is vlan4.

NOTE

- Since the convergence of the RPF routing that works with PIM and BFD also depends on the convergence rate of unicast routing, BFD is also required to work with relevant unicast routing protocol OSPF.

53 Hardware QoS

53.1 Overview

53.1.1 Background

In the traditional IP network, the forwarding device treats all packets equally, adopts “First in, first out” (FIFO) to process all packets and tries best effort to transmit the packet to the destination, so it cannot provide any guarantee for the reliability and delay of the packet transmission.

However, with the development of the IP network, the new applications based on the IP network emerge in endlessly, which put forward new requirements for the service quality of the IP network, especially the demand for the service packets with high real-time requirement is more obvious. For example, the network flow media, VoIP and other real-time services put forward high requirement for the transmission delay of the packets. If the packet transmission delay is long, the user cannot accept (relatively, E-mail and FTP services are not sensitive to the transmission delay). To support the communication services with different service quality requirements, it is required that the network can intelligently distinguish different communication types, so as to provide the corresponding service. The capability of distinguishing the communication types is the basic premise of providing different service qualities for different communications, so the best-effort service mode of the traditional IP network cannot meet the requirements of the present IP network application. The QoS (Quality of Service) technology is to solve the problem, so as to meet the different service quality requirements of the users for the network.

53.1.2 Service Model

QoS provides the following three kinds of service models, that is, Best-Effort service, Integrated service, and Differentiated service (DiffServ for short).

Best-Effort is a single service model and also the simplest service model. The application program can send out any quantity of packets at any time without getting the permission or informing the network in advance. For the best-effort service, the network tries best to send the packets, but does not provide ant guarantee for the transmission delay and reliability of the packets. Best-Effort is the default service model of Internet and is applicable to most of network applications, such as FTP and E-Mail. It is realized via the FITO queue mechanism.

IntServ is one service model that can provide various service types. It can meet various QoS requirements. Before sending packets, the service model needs to apply for the specified service resources from the network. The request is completed via the RSVP signaling. RSVP applies for the network resources for the application before the application program starts to send packets, so it belongs to the out-band signaling. Before sending data, the application program first informs the network of its own traffic parameters and the needed specified service quality request, including bandwidth, delay and so on. After receiving the resource request of the application program, the network executes the resource distributing check, that is, judge whether to distribute resources for the application program based on the resource application of the application program and the present resources of the network. Once the network confirms to distribute resources for the application program, the network maintains one state for the specified flow (Flow, confirmed by the IP addresses, port numbers and protocol numbers of the two sides) and executes the packet classification, traffic monitoring, queuing and scheduling based on the state. After receiving the confirming information of the network (that is, confirm that the network already reserves resources for the packets of the application program), the application program can send packets. As long as the packets of the application program are controlled within the range described by the traffic parameters, the network will undertake to meet the QoS requirements of the application program.

DiffServ classifies the communications according to the service requirements, and then processes the ingress and egress packets according to the classification result, so as to ensure that the network is always in the good communication connection status. It is one multi-channel service model and can meet the QoS requirements of different flows. The largest difference with IntServ is that DiffServ can reserve resources in the network without signaling exchange. It just functions on one port of one transmission device in the network, processing the ingress and egress packets of the port. DiffServ does not need to maintain the status information for each kind of communication. It distinguishes the QoS level of each packet according to the configured QoS mechanism and provides the service for the packet according to the level. Therefore, the mechanism providing the QoS scheme is also called CoS. There are many classification methods and the common modes are to classify according to the priority of the IP packet, classify according to the source, destination address and port of the packet, classify according to the packet protocol, classify according to the packet size and packet ingress port, and so on.

Priority mapping, flow classification, traffic monitoring, traffic shaping, congestion management and congestion avoidance are the main components of DiffServ. The flow classification identifies the packets according to some matching rules and is the basis and premise of DiffServ; traffic monitoring, traffic shaping, congestion management and congestion avoidance distribute and schedule the resources for the network traffic from different aspects and they are the embodiment of the DiffServ idea.

53.1.3 Introduction to QoS Functions *-B -S -E -A*

Priority Mapping

Priority mapping includes the ingress mapping and egress mapping. Ingress mapping maps to the local priority (LP) according to the 802.1p priority and DSCP value in the packet; egress mapping maps to the 802.1p priority and DSCP value according to the local priority (LP) of the packet. Priority mapping serves for the queue scheduling and congestion control.

The device supports seven kinds of priority mapping: map the packet DSCP to the local priority (LP); map the ingress DSCP value of the packet to the egress DSCP value of the packet; map the 802.1p priority of the packet to the local priority (LP); map the 802.1p priority of the packet to the egress DSCP value; map the local priority (LP) of the packet to the egress 802.1p priority of the packet; map the local priority (LP) of the packet to the egress DSCP value of the packet; map the local priority of the packet (LP) to the egress queue. The diagram of the priority mapping relation is as follows:

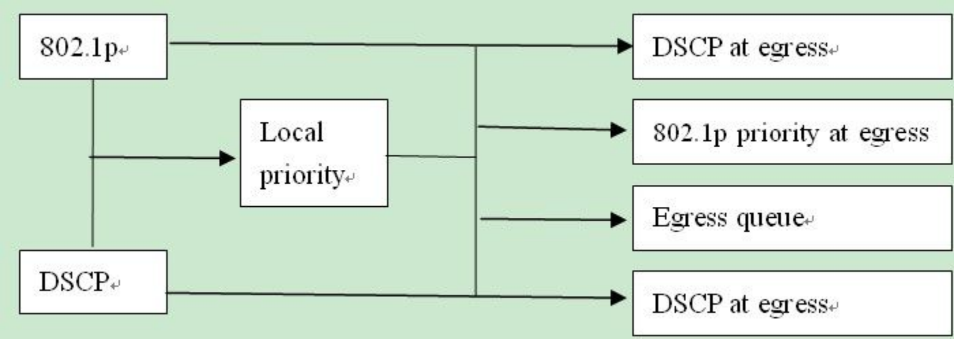


Figure 1-1Diagram of priority mapping relation

Flow Classification

Flow classification adopts some rule to identify the packets that comply with one feature, divides the packets of different features to multiple classes, and then uses the corresponding QoS mechanism to provide different services for different classes. Therefore, the flow classification is the premise and basis of providing different services.

Flow classification includes counter, meter, flow mirror, re-direction and re-remarking.

Counter and meter perform the counting and metering actions according to the result of the flow classification.

Flow mirror means to mirror the matched packets to the specified ports.

Re-direction means to re-direct the matched packets to the specified port or the specified next hop.

Re-marking means to set or modify the attributes of one kind of packets. After dividing the packets to different kinds via the flow classification, re-marking can modify the attributes of the packet. Prepare for the subsequent processing of the packet.

Traffic Monitoring

Traffic monitoring limits the speed of the ingress packets via the token bucket. To ensure that the overload does not happen to the traffic passing the network and causes the congestion, the device provides the rate limitation based on the port receiving direction, limiting the total rate at the receiving direction of the port. The speeding traffic is dropped.

Traffic Shaping

The typical function of the traffic shaping means to limit the traffic of flowing out from one network, making the packets sent with an average rate. Usually, it is divided to the port traffic shaping and queue traffic shaping. When the sending rate of the packets exceeds the shaping rate, the speeding packets are buffered in the queue and then are sent out with an average rate. The difference between the traffic shaping and traffic monitoring: When using the traffic monitoring to control the packet traffic, the speeding packets are not buffered, but are directly dropped, while the traffic shaping buffers the speeding packets, reducing the dropped packets caused by the burst traffic. However, the traffic shaping may increase the delay, while the traffic monitoring nearly does not increase the delay.

Congestion Management

When the device traffic load is light, do not generate the congestion and the packets are forwarded out when reaching the port. When the arriving rate of the packets is larger than the sending rate of the port and exceeds the processing limit of the port or the device resources are not enough, congestion happens to the device. The congestion may make the communication of the whole network become unreliable. The end-to-end delay, jitter and packet loss rate used to measure the network service quality all increase. If enabling the congestion management and when the congestion happens, the packets queue at the port and waits for the port to forward. The congestion management usually adopts the queue technology and the port determines which queue the packet should be placed according to the packet priority and queue mechanism and how to schedule and forward packets.

The common scheduling includes SP (Strict Priority), RR (Round Robin), WRR (Weighted Round Robin), and WDRR (Weighted Deficit Round Robin).

SP (Strict Priority): There are eight queues on the port, queue 0-7. Queue 7 has the highest priority and queue 0 has the lowest priority.

RR (Round Robin): After one queue schedules one packet, turn to the next queue.

WRR (Weighted Round Robin): It is the weighted scheduling based on packet. You can configure the number of the packets scheduled by each queue before turning to the next queue.

WDRR (**Weighted Deficit Round Robin)**: It is the improvement for the WRR algorithm. The algorithm is based on two variables, that is, quantum and credit counter. The quantum means the weight in the unit of byte and it is a configurable parameter. The credit counter means the accumulation and consumption of the quantum, which is a status parameter and cannot be configured. In the initial state, the credit counter of each queue is equal to the quantum. Every time the queue sends a packet, subtract the byte number of the packet from the credit counter. When the credit counter is lower than 0, stop the scheduling of the queue. When all queues stop scheduling, supplement quantum for all queues.

Congestion Avoidance

The congestion avoidance technology monitors the communication load of the network, so as to avoid the congestion before the network congestion happens. The common used technology is WRED (Weighted Random Early Detection). The difference with the tail drop method is that WRED selects the dropped packet according to the DSCP or IP priority and can provide different performance features for different service types of data. It also can avoid the TCP global synchronization.

In the WRED algorithm, the start point of the queue drop packet is marked as DropStartPoint and the end point of the drop is marked as DropEndPoint. When the average length of the queue is between DropStartPoint and DropEndPoint, WRED drops the packet at random by the corresponding drop rate, while when the queue length exceeds DropEndPoint, drop the packet by 100%. When the queue length is smaller than DropStartPoint, WRED does not drop the packet.

The following is the diagram of the WRED:

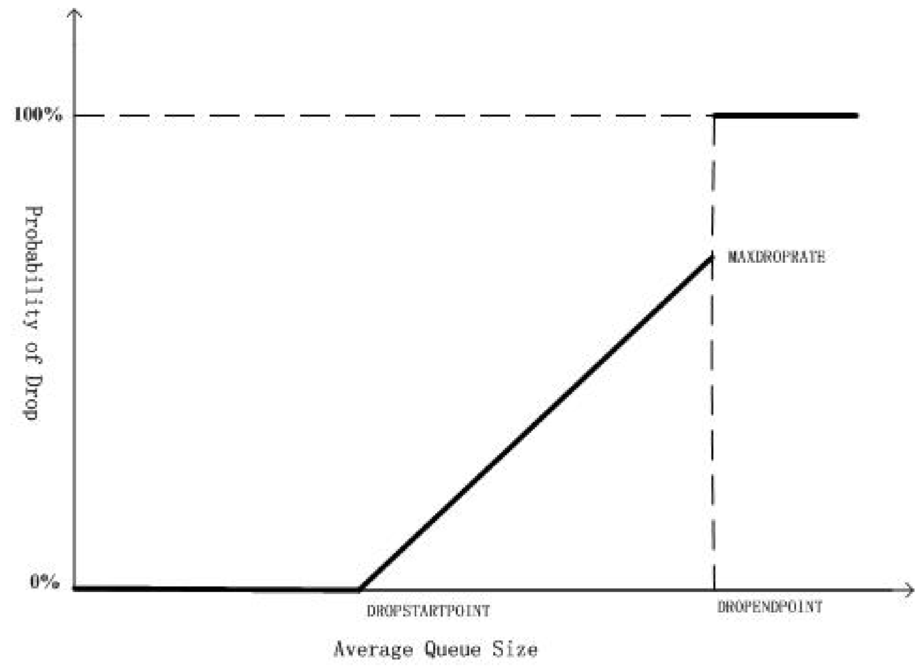


Figure 1-2 WRED diagram

Action Group Function

To support the flow classification and traffic control, the device extends the traditional ACL so that ACL and ACL rule can be bound with one action group respectively, adopting the corresponding action for the matched packet. The action group contains the configurations of the counter, meter, flow mirror, re-direction and re-marking.

For various ACLs and ACL rules being used in different function domains, the configurations of the action groups are different. For the ingress ACL, the used action group of IP ACL is L3 action group and the used action group of MAC ACL is L2 action group. The egress action group is used at the egress direction of ACL. The VFP action group is used to realize the flow-based QinQ. Each ACL can be bound with various action groups, but the effective one depends on the function domain bound with the ACL. For example, one rule of IP ACL is configured with L3 action group, egress action group and VFP action group at the same time. When the IP ACL is applied at the ingress direction, the action in the L3 action group take effect and the actions in the other two action groups do not take effect.

The policy route in the action group is one packet forwarding mechanism for flexible routing based on the destination network. The policy route classifies the packets via Content Aware Processor and forwards the data flow that complies with the classification rule according to the specified next hop. When some packet is routed by other path, but not the shortest path, we can enable the policy route. The priority of the policy route is higher than any other route. Therefore, once the user configures enabling the policy route, the packet sending is processed according to the policy route. Only when the access list matching fails, we can continue to forward according to the searching result of the forwarding table. Otherwise, forward the packet according to the specified next-hop information of the route policy. The specified next hop of the policy route should be the direct-connected next hop. For the non-direct-connected next-hop address, the system permits to configure, but in fact, it is invalid.

VLAN QoS Function

VLAN-based QoS is to map the data flow of some VLAN to 16 virtual queues, and then schedule and shape the 16 virtual queues.

The following is the principle of realizing the VLAN queue shaping.

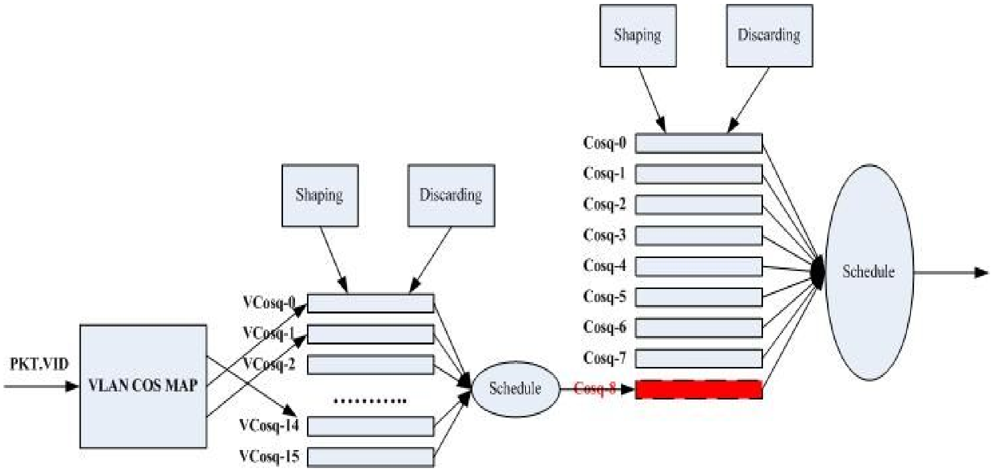


Figure 1-3 VLAN QoS diagram

After the device receives the data flow, first map the data flow to different VLAN QoS virtual queues according to the VLAN ID in the packet VLAN tag, and then realize the VLAN QoS queue scheduling and shaping on the virtual queues. After VLAN QoS scheduling and shaping, the traffic enters queue 9 of the port.

53.2 Hardware QoS Function Configuration

Table 1-1 The configuration list of the hardware QoS function

Configuration task	
Configure the priority mapping	Configure the priority mapping
	Configure the default priority mapping
	Configure the global priority mapping
	Configure reserving 802.1p priority
Configure the flow classification	Configure the counter
	Configure the meter
	Configure the flow mirror
	Configure the re-direction
	Configure re-marking l2-priority
	Configure re-marking l3-priority

Configuration task	
Configure the traffic monitoring	Configure the port-based rate limitation
Configure the traffic shaping	Configure the queue-based traffic shaping
	Configure the port-based traffic shaping
Configure the congestion management	Configure the scheduling policy of the port queue
Configure the congestion avoidance	Configure the drop mode
Configure the VFP action group	Configure the processing for the packet with a single-layer VLAN tag
	Configure the processing for the packet with double-layer VLAN tag
	Configure the processing for the packet without VLAN tag
	Configure binding VRF in the VFP action group
Configure VLAN QoS	Configure the VLAN QoS mapping
	Configure the VLAN QoS scheduling
	Configure the VLAN QoS shaping
Configure the broadcast packet shielding	Configure the broadcast packet shielding

53.2.1 Configure Priority Mapping *-B -S -E -A*

Priority mapping is the mapping among the 802.1p priority, DSCP value and local priority (LP) in the packet. Modify or distribute the priority field of the packet to serve for the congestion avoidance and congestion management.

Configuration Condition

None

Configure Priority Mapping

Priority mapping includes the ingress mapping and egress mapping. The ingress mapping maps to the local priority (LP) according to the 802.1p priority and DSCP value in the packet; the egress mapping maps to the 802.1p priority and DSCP value according to the local priority (LP).

Table 1-1 Configure the priority mapping

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port.; After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the priority mapping	**map-table** { **dot1p-dscp** | **dot1p-lp** | **dscp-dscp** | **dscp-lp** | **lp- dot1p** | **lp-dscp** } *index* **to** *value*	Mandatory By default, the priority mapping is not configured.

NOTE

- For the packet with the specified priority entering the queue, you'd better not let the packet enter queue 7, because the packets sent out from CPU all enter queue 7. If queue 7 has too many packets, the packets from CPU may be dropped.
- The dscp-lp mapping and dotlp-lp are configured on the port at the same time. The dscp-lp has higher priority and it takes effect first.
- After configuring any mapping of the dscp-dscp mapping and if not configuring the default dscp-dscp priority mapping, the other entries not configuring the dscp-dscp mapping under the port are mapped to the DSCPs with the same value. If the default dscp-dscp mapping is configured, the un-configured items are mapped to the default value. After configuring DSCP-DSCP mapping, enable the DSCP-LP mapping automatically. Once any dscp-lp mapping is configured on the port, the un-configured items are mapped to different LPs by section. The mapping relationship is as follows: the value of dscp from 0 to 7 is mapped to lp value 0; the value of dscp from 8 to 15 is mapped to lp value 1, and the following values are accounted as the above way. If the input is UNTAG packet, the 802.1P priority in the output packet VLAN Tag is modified according to dscp-lp mapping;
- After enabling the ingress dot1p-lp mapping, the 802.1p priority of the forwarded packet is modified according to the local priority (LP) by default. For example, the dot1p-lp

mapping relation is 1 to 5; after matching the 802.1p of the VLAN Tag in the ingress packet to 1, the 802.1p priority of the forwarded packet with VLAN Tag is modified to 5.

- The priority mapping does not take effect for the packet remarked by the action group. First, remark the local priority (LP) at the ingress action group, and then mapping to the 802.1p priority and DSCP value of the packet via the local priority (LP) at the egress takes effect. Remark the 802.1p priority at the ingress and then mapping the local priority and DSCP value via the 802.1p priority does not take effect, but remarking the 802.1p priority itself takes effect. Mapping according to the 802.1p priority of the original packet also takes effect, that is to say, remarking takes effect separately, the priority mapping takes effect separately, and the priority mapping according to the remarked value does not take effect.
- When the ingress DSCP-DSCP and egress LP-DSCP are configured at the same time, the two mappings take effect by LP-DSCP mapping.
- If the QINQ function is enabled on the port, and you enable dot1p-lp, dscp-dscp, and dscp-lp mappings again, maybe you cannot get the desired mapping result. Therefore, it is recommended not to enable QINQ and priority mapping functions on one port at the same time.
- After configuring the lp-dscp mapping, the default mapping of lp-dscp is 0 to 7, 1 to 8, 2 to 16, 3 to 24, 4 to 32, 5 to 40, 6 to 48, and 7 to 56.

Configure Default Priority Mapping

The default priority mapping, the same as the priority mapping, has the ingress and egress mapping. The difference lies in that the default priority mapping maps the entries not configured with priority mapping to the default value.

Table 1-2 Configure the default priority mapping

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port.; After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the default priority mapping	**map-table default** { **dot1p-dscp** | **dot1p-lp** | **dscp-dscp**	Mandatory

Step	Command	Description
	| **dscp-lp** | **lp- dot1p** | **lp-dscp** } *value*	By default, the default priority mapping is not configured.

Configure Global Priority Mapping

The global priority mapping maps the local priority mapping to the egress queue. After configuring the global priority mapping, the packets received from all ports are mapped to the egress queue according to the local priority.

Table 1-3 Configure the global priority mapping

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the global priority mapping	**map-table lp-cosq** *index* **to** *value*	Mandatory By default, the global priority mapping is not configured.

Configure Reserved 802.1p Priority

Configure the reserved 802.1p priority on the port to prevent the 802.1p priority in the packets received from the port from being changed by any policy. When the reserved 802.1p priority is not configured, the packets received from the port will modify the 802.1p value according to the priority mapping and re-marking. For example, after the ingress dot1p-lp mapping is enabled, the 802.1p priority for forwarding packets will be modified according to the local priority value; if the reserved 802.1p priority is configured, the 802.1p priority for forwarding packets will not be modified according to the local priority value.

Table 1-4 Configure the reserved 802.1p priority

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		current port.; After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure the reserved 802.1p priority	**preserve dot1p**	Mandatory By default, the reserved 802.1p priority is not configured.

53.2.2 Configure Flow Classification *-B -S -E -A*

Flow classification adopts some rule to identify the packets that comply with one feature, divides the packets of different features to multiple classes, and then uses the corresponding QoS mechanism to provide different services for different classes. Therefore, the flow classification is the premise and basis of providing different services.

Configuration Condition

Before configuring the flow classification, first complete the following task:

- Configure the ACL.

Configure Counter

Configuring counting action in the action group aims to count the number of the matched packets.

Table 1-5 Configure the counter

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the L3 action group and enter the L3 action group configuration mode	**l3-action-group** *l3-action-group-name*	Either After entering the L3 action group configuration mode, the subsequent configuration just takes effect in the current L3 action group; After entering the L2 action group configuration mode,
Configure the L2 action group and enter the L2 action group configuration mode	**l2-action-group** *l2-action-group-name*	

Step	Command	Description
Configure the egress action group and enter the egress action group configuration mode	**egr-action-group** *egr-action-group-name*	the subsequent configuration just takes effect in the current L2 action group; After entering the egress action group configuration mode, the subsequent configuration just takes effect in the current egress action group
Configure the counter	**count** { **all-colors** | **green-other** | **green-red** | **green-yellow** | **red-other** | **red-yellow** }	Mandatory By default, packets are not counted in the action group.

Configure Meter

Configure the meter in the action group to limit the rate or mark the matched packets. When configuring a nonexistent meter, the meter takes effect immediately when the specified meter is configured. When no meter is configured in the action group, all matched packets are considered as green packets. When a meter is configured in the action group for coloring the packets, the packets will be marked in green, yellow, and red according to the packet traffic, and then the counter will count the number of the packets of different colors.

Table 1-6 configure the meter

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the meter and enter the meter mode	**traffic-meter** *traffic-meter-name*	Mandatory By default, the packets in red and yellow are dropped and the meter mode is not configured. After entering the meter configuration, a complete meter configuration contains meter actions for packets in red and yellow and meter mode configuration. An incomplete configuration will not take effect.

Step	Command	Description
Configure the meter actions	**meter action** { **red** | **yellow** } { **drop** | **transmit** [**remark-dot1p** *priority-value* [**remark-dscp** *dscp-value*] | **remark-dot1p-lp** *priority-value* [**remark-dscp** *dscp-value*] | **remark-dscp** *dscp-value* | **remark-1p** *priority-value* [**remark-dscp** *dscp-value*] }	Optional By default, the packets in red and yellow are dropped.
Configure the meter mode	**meter mode** { **srtcm** *cir cbs ebs* | **trtcm** *cir cbs pir pbs* }	Mandatory By default, the meter mode is not configured.
Enter the global configuration mode	**exit**	-
Configure the L3 action group and enter the L3 action group configuration mode	**l3-action-group** *l3-action-group-name*	Either After entering the L3 action group configuration mode, the subsequent configuration just takes effect in the current L3 action group; After entering the L2 action group configuration mode, the subsequent configuration just takes effect in the current L2 action group; After entering the egress action group configuration mode, the subsequent configuration just takes effect in the current egress action group
Configure the L2 action group and enter the L2 action group configuration mode	**l2-action-group** *l2-action-group-name*	
Configure the egress action group and enter the egress action group configuration mode	**egr-action-group** *egr-action-group-name*	
Configure the binding meter	**meter** *traffic-meter-name*	Mandatory By default, no meter is bound.

NOTE

- If the ACL bound to the objects is configured with the action group and the action group is configured with a meter for limiting the rate, conflicted rate limitation actions may exist. When the rate limitation is applied, the packets in red and yellow are dropped. For example, port 0/1 belongs to VLAN1, the ACL on port 0/1 permits the packets of the source IP address 1.1.1.1 to pass, and the traffic is configured within 5 Mbps. The ACL of VLAN1 permits the packets of the source IP address 1.1.1.1 to pass and the traffic is configured within 1 Mbps. In this situation, the minimum rate in the packet channel will take effect and the traffic is configured within 1 Mbps. Specially, due to the hardware limitation, the actual traffic for multi-level rate limitation will be less than the minimum rate in the packet channel. Therefore, multi-level rate limitation is not recommended when an accurate rate limitation is needed.
- The meter in the egress action group does not support the remark Ip or remark dotlp-Ip action.
- The meter is based on the chips. That is, the meter on each chip limits the traffic rate over the port. If the meter exists in two different chips under the link aggregation port, a meter exists in each chip and thus the rate limitation has the effect twice of the expected rate limitation effect.
- If a meter is applied to the VLAN, the meter takes effect for each chip on each line card. VLAN objects are limited within 10 Mbps. If five single-core line cards exist on the device, the 10 Mbps traffic takes effect for a pair of line cards. That is, the traffic on each line card complying with the VLAN rate limitation is 10 Mbps. If two chips exist on a line card, the traffic for each chip on the line card is 10 Mbps.

Configure Flow Mirror

Configuring the flow mirror in the action group aims to specify the matched packet to the port.

Table 1-7 Configure the flow mirror

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the L3 action group and enter the L3 action group configuration mode	**l3-action-group** *l3-action-group-name*	Either After entering the L3 action group configuration mode, the subsequent configuration just takes effect in the current L3 action group; After entering the L2 action group configuration mode, the subsequent configuration just takes effect in the current L2 action group.
Configure the L2 action group and enter the L2 action group configuration mode	**l2-action-group** *l2-action-group-name*	
Configure the flow mirror	**mirror interface** *interface-name*	Mandatory

Step	Command	Description
		By default, the flow mirror is not configured.

Configure Re-direct

Configuring the packet re-direct in the action group aims to redirect the matched packets to the specified port or the specified next hop.

Table 1-8 Configure the re-direct

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the L3 action group and enter L3 action group configuration mode	**l3-action-group** *l3-action-group-name*	Either After entering the L3 action group configuration mode, the subsequent configuration just takes effect in the current L3 action group; After entering the L2 action group configuration mode, the subsequent configuration just takes effect in the current L2 action group.
Configure the L2 action group and enter the L2 action group configuration mode	**l2-action-group** *l2-action-group-name*	
Configure the re-direct	**redirect** { **interface** *interface-name* | **ipv4-nexthop** *ip-address* [*ip-address*] [*ip-address*] [*ip-address*] [*ip-address*] [*ip-address*] }	Mandatory By default, the packet re-direct is not configured.

Configure Re-marking l2-priority

Configuring packet re-marking in the action group aims to classify the matched packets to facilitate users to adopt different QoS policies in the subsequent data communications.

Table 1-9 Configure re-marking l2-priority

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the L3 action group and enter the L3 action group configuration mode	**l3-action-group** *l3-action-group-name*	Either After entering the L3 action group configuration mode, the subsequent configuration just takes effect in the current L3 action group; After entering the L2 action group configuration mode, the subsequent configuration just takes effect in the current L2 action group; After entering the egress action group configuration mode, the subsequent configuration just takes effect in the current egress action group
Configure the L2 action group and enter the L2 action group configuration mode	**l2-action-group** *l2-action-group-name*	
Configure the egress action group and enter the egress action group configuration mode	**egr-action-group** *egr-action-group-name*	
Configure re-marking l2-priority	**remark l2-priority** { **dot1p** | **dot1p-lp** | **lp** } { *priority-value* | **precedence** }	Mandatory By default, re-marking l2-priority is not configured.

Configure Re-marking l3-priority

Configuring packet re-marking in the action group aims to classify the matched packets to facilitate users to adopt different QoS policies in the subsequent data communications.

Table 1-10 Configure re-marking l3-priority

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the L3 action group and enter the L3 action group configuration mode	**l3-action-group** *l3-action-group-name*	Either After entering the L3 action group configuration mode, the subsequent configuration just takes effect in the current L3 action group; After
Configure the egress action group and enter the	**egr-action-group** *egr-action-group-name*	

Step	Command	Description
egress action group configuration mode		entering the egress action group configuration mode, the subsequent configuration just takes effect in the current egress action group.
Configure re-marking l3-priority	**remark l3-priority** { **dscp** *dscp-value* | **precedence** { *priority-value* | **dot1p** } }	Mandatory By default, re-marking l3-priority is not configured.

NOTE

- If the ACL bound to the objects is configured with the action group, re-marking confliction may exist. For example, port 0/1 belongs to VLAN1, the ACL on port 0/1 permits the packets of the source IP address 1.1.1.1 to pass, and the action for re-marking the DSCP field as 5 is configured. The ACL of VLAN1 permits the packets of the source IP address 1.1.1.1 to pass and the action for re-marking the DSCP field as 4 is configured. In this situation, this situation is handled based on port > VLAN > global and MAC ACL > IP ACL by priority and the final re-marking value is 5.
- If the ACL bound to the objects is configured with the action group, conflict-free re-marking action may exist. For example, port 0/1 belongs to VLAN1, the ACL on port 0/1 permits the packets of the source IP address 1.1.1.1 to pass, and the action for re-marking the DSCP field as 5 is configured. The ACL of VLAN1 permits the packets of the source IP address 1.1.1.1 to pass and the 802.1p priority is re-marked as 4. For the conflict-free re-marking action, the packet DSCP will be marked as 5 and the 802.1p priority will be marked as 4.

53.2.3 Configure Traffic Monitoring *-B -S -E -A*

To ensure that the overload does not happen to the traffic passing the network and causes the congestion, the device provides the rate limitation based on the port receiving direction, limiting the total rate at the receiving direction of the port. The speeding traffic is dropped.

Configuration Condition

None

Configure Port-based Rate Limitation

To provide different rate limitations for ports at different time periods, each port is configured with eight rate limitations of different priorities. Each rate is limited and then bound to a time domain. For the entries taking effect at the same time, determine which entry takes effect by priority. The number 0 indicates the highest priority and the number 7 indicates the lowest priority. The rate limitation over the port can be configured directly without the time domain.

Table 1-11 Configure port-based rate limitation

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure port-based rate limitation	**rate-limit** { **default** *rate burst-size* | *priority rate burst-size* [**time-range** *time-range-name*] }	Mandatory By default, rate limitation over the port is not configured.

53.2.4 Configure Traffic Shaping *-B -S -E -A*

The traffic shaping enables the packets to be sent out at an average rate. The difference between the traffic shaping and traffic monitoring: the traffic monitoring takes effect in the ingress direction and the traffic shaping takes effect in the egress direction. The excessive traffic at the ingress direction will be dropped, but the excessive traffic at the egress direction will be cached.

Configuration Condition

None

Configure Queue-based Traffic Shaping

Queue-based traffic shaping enables the traffic in the queue to be sent out at an average rate. Different traffic shaping can be performed for different queues as required.

Table 1-12 Configure queue-based traffic shaping

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure queue-based traffic shaping	**traffic-shape queue** *queue-id cir cbs pir pbs*	Mandatory By default, queue-based traffic shaping is not configured.

Configure Port-based Traffic Shaping

The port-based traffic shaping allows the time domain binding to achieve different bandwidths in different time periods. Each port is configured with eight traffic shaping of different priorities and each traffic shaping is bound to a time domain. For the entries taking effect at the same time, determine which entry takes effect by priority. The number 0 indicates the highest priority and the number 7 indicates the lowest priority.

Table 1-13 Configure the port-based traffic shaping

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the port-based traffic shaping	**traffic-shape** { *rate burst-size* | *priority rate burst-size* [**time-range** *time-range-name*] }	Mandatory By default, port-based traffic shaping is not configured.

53.2.5 Configure Congestion Management *-B -S -E -A*

In a complex network, congestion is common because the current bandwidth cannot satisfy the normal forwarding. Congestion may cause a series of negative problems as follows: the system breaks down because of abundant network resources, the network resource utility is low because of decreased network throughput, and packet transmission delay and jitter increase. Scheduling policy for the port queue is a method for managing the congestion.

Configuration Condition

None

Configure Scheduling Policy of Port Queue

The queue-based scheduling policy sends out the classified traffic by a certain priority-level algorithm. Each queue algorithm solves a certain network traffic problem and has great influence on bandwidth resource allocation, delay, and jitter. Queue scheduling processes the packets of different priorities in levels. A packet with high priority will be sent preferentially.

The common scheduling includes SP (Strict Priority), RR (Round Robin), WRR (Weighted Round Robin), and WDRR (Weighted Deficit Round Robin).

SP (Strict Priority): There are eight queues on the port, queue 0-7. Queue 7 has the highest priority and queue 0 has the lowest priority.

RR (Round Robin): After one queue schedules one packet, turn to the next queue.

WRR (Weighted Round Robin): It is the weighted scheduling based on packet. You can configure the number of the packets scheduled by each queue before turning to the next queue.

WDRR (Weighted Deficit Round Robin): It is the improvement for the WRR algorithm. The algorithm is based on two variables, that is, quantum and credit counter. The quantum means the weight in the unit of byte and it is a configurable parameter. The credit counter means the accumulation and consumption of the quantum, which is a status parameter and cannot be configured. In the initial state, the credit counter of each queue is equal to the quantum. Every time the queue sends a packet, subtract the byte number of the packet from the credit counter. When the credit counter is lower than 0, stop the scheduling of the queue. When all queues stop scheduling, supplement quantum for all queues.

Table 1-14 Configure the scheduling policy for the port queue

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the scheduling policy for the port queue	**queue-schedule** { **sp** | **rr** | { { **wrr** | **wdrr** } *weight0 weight1 weight2 weight3 weight4 weight5 weight6 weight7* [*weight8*] } }	Mandatory By default, the scheduling policy for the port queue is the SP.

53.2.6 Configure Congestion Avoidance *-B -S -E -A*

The congestion avoidance technology monitors the network resource utility and communication load of the network, so as to avoid the congestion by actively dropping packets before the network congestion happens or worsens. Excessive congestion exerts great harm on network resources and therefore, a certain measure must be adopted to relieve the congestion. The common measure is to configure the packet drop mode.

Configuration Condition

None

Configure Drop Mode

Tail drop and WRED (Weighted Random Early Detection) are two common packet drop modes.

Tail drop: It is a traditional packet drop policy. When the queue length reaches the maximum value, all new packets will be dropped. This packet drop policy may cause TCP global synchronization. When the packets connected by multiple TCPs are dropped in a queue, multiple TCP connections will enter the congestion avoidance and slow-start status to decrease and adjust the traffic, and then the traffic peak may occur simultaneously at a time. Repeatedly, the traffic and network are unstable.

WRED: When the queue length exceeds its own length, the packets are dropped by 100%. When the queue length is less than the start-value, do not drop any packet. When the queue length is greater than the start-value, drop packets at random according to the configured value. The random number generated by the WRED is based on the priority. The WRED introduces the IP priority to distinguish from the packet drop policy. The packet with high priority is considered for its benefit and this packet will be dropped in a relatively low probability.

Table 1-15 Configure the packet drop mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the drop mode	**drop-mode** *cos-value* { **tail-drop** | **wred drop-start** start-value **drop-rate** drop-rate-value [**only-tcp** | **all**] }	Mandatory By default, the packet drop mode for the port queue is the tail drop mode.

53.2.7 Configure VFP Action Group *-B -S -E -A*

VFP (VLAN Filter Processor) action group classifies the packets and then specifies the packet with the single-layer VLAN tag, the packet with double-layer VLAN tag, and the packet without VLAN tag.

Configuration Condition

Before configuring the VFP action group, first complete the following task:

- Configure the ACL.

Configure Processing for the Packet with Single-layer VLAN Tag

In the VFP action group, configure the processing for the packet with single-layer VLAN tag, especially for matching and processing the 802.1p priority and VLAN numbers in the VLAN tag.

Table 1-16 Configure the processing for the packet with single-layer VLAN tag

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the VFP action group and enter the VFP	**vfp-action-group** *vfp-action-group-name*	Mandatory

Step	Command	Description
action group configuration mode		By default, the VFP action group is not configured.
Configure the processing for the packet with single-layer VLAN tag	**one-tag** { **match-vlan** { **any** | *vlan-id* } | **ovlan-act** { **add-ovlan** *vlan-id* [**priority** *priority-value*] } | **replace-vlan** *vlan-id* }	Mandatory By default, the processing for the packet with single-layer VLAN tag is not configured.

Configure Processing for Packet with Double-layer VLAN Tag

In the VFP action group, configure the processing for the packet with double-layer VLAN tag, especially for matching and processing the 802.1p priority and VLAN numbers in the inner and outer VLAN tag.

Table 1-17 Configure the processing for the packet with double-layer VLAN tag

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the VFP action group and enter the VFP action group configuration mode	**vfp-action-group** *vfp-action-group-name*	Mandatory By default, the CFP action group is not configured.
Configure the processing for the packet with double-layer VLAN tag	**double-tag** { **invlan-act** { **delete-invlan** | **replace-invlan** *vlan-id* } | **match-invlan** { **any** | *vlan-id* } | **match-ovlan** { **any** | *vlan-id* } | **ovlan-act replace-ovlan** *vlan-id* }	Mandatory By default, the processing for the packet with double-layer VLAN tag is not configured.

Configure Processing for Packet without VLAN Tag

In the VFP action group, configure the processing for the packet without VLAN tag, especially for adding the inner and outer VLAN tag.

Table 1-18 Configure the processing for the packet without VLAN tag

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Configure the VFP action group and enter the VFP action group configuration mode	**vfp-action-group** *vfp-action-group-name*	Mandatory By default, the VFP action group is not configured.
Configure the processing for the packet without VALN tag	**untag** { **invlan-act add-invlan** *vlan-id* } | **ovlan-act add-ovlan** *vlan-id*	Mandatory By default, the processing for the packet without VLAN tag is not configured.

Configure Binding VRF in VFP Action Group

Table 1-19 Configure binding VRF in the VFP action group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the VFP action group and enter the VFP action group configuration mode	**vfp-action-group** *vfp-action-group-name*	Mandatory By default, the VFP action group is not configured.
Configure binding VRF in the VFP action group	**vrfset** *vrf-name*	Mandatory By default, binding VRF in the VFP action group is not configured.

53.2.8 Hardware QoS Monitoring and Maintaining *-B -S -E -A*

Table 1-20 Hardware QoS monitoring and maintaining

Command	Description
show drop-mode [**interface** *interface-name*]	Display the drop mode of the port queue
show egr-action-group [*egr-action-group-name*]	Display related configuration information of the egress action group

Command	Description
show flood-control interface *interface-name*	Display the broadcast frame shielding information of the specified port
show l2-action-group [*l2-action-group-name*]	Display the related configuration information of the L2 action group
show l3-action-group [*l3-action-group-name*]	Display the related configuration information of the L3 action group
show map-table { **all** | { **dot1p-dscp** | **dot1p-lp** | **dscp-dscp** | **dscp-lp** | **lp- dot1p** | **lp-dscp** } [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*] }	Display the priority mapping information
show preserve dot1p	Display the reserved 802.1p priority information on the port
show queue-schedule [**interface** *interface-name*]	Display the scheduling policy of the port queue
show rate-limit [**interface** *interface-name*]	Display the rate limitation information of the port
show traffic-count { **inst-all** | **inst-global** | { **inst-interface** *interface-name* | **inst-link-aggregation** *link-aggregation-id* } { **ip-in** | **ip-out** | **mac-in** | **mac-out** } | **inst-vlan** *vlan-id* {**ip-in** | **ip-out** }}	Display the counter information of the ACL applied to the specified port
show traffic-meter [*traffic-meter-name*]	Display all counter information
show traffic-shape [**interface** *interface-name*]	Display the traffic shaping information on the port and in the queue
show vfp-action-group [*vfp-action-group-name*]	Display related configuration information in the VFP action group
show vlan-map	Display the configuration information of mapping the specified VLAN data flow to the 16 virtual queues
show vlanq-shape [**interface** *interface-name*]	Display the configuration information of VLAN shaping

Command	Description
show vlanshape-sus-port [*slot-number*]	Display the ports on the specified slots supporting VLAN QoS

53.3 Typical Configuration Example of Hardware QoS

53.3.1 Configure Priority Mapping *-B -S -E -A*

Network Requirements

- There are two servers in the network, that is, Video server and Data server.
- The DSCP value in the video traffic packet is 34 and the DSCP value in the data traffic packet is 38.
- Configure the priority mapping function, realizing that the 802.1p priority of the video traffic packet is 5 and the 802.1p priority of the data traffic packet is 1.

Network Topology

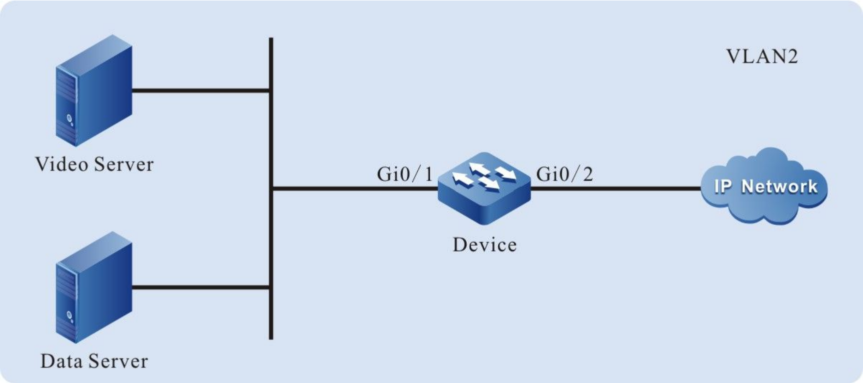


Figure 53-2 Networking of configuring the priority mapping

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 as Trunk and permit the services of VLAN2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the priority mapping function.

#Configure the priority mapping function on port gigabitethernet0/1, map the packet with DSCP value 34 to queue 2 and map the packet with DSCP value 38 to queue 3.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#map-table dscp-lp 34 to 2
Device(config-if-gigabitethernet0/1)#map-table dscp-lp 38 to 3
```

#Configure the priority mapping function on port gigabitethernet0/2, map the 802.1p priority of the packet in queue 2 to 5 and map the 802.1p priority of the packet in queue 3 to 1.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#map-table lp-dot1p 2 to 5
Device(config-if-gigabitethernet0/2)#map-table lp-dot1p 3 to 1
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Check the result.

#After the video traffic and data traffic are processed by Device, the 802.1p priority of the video traffic packet sent out from port gigabitethernet0/2 is 5 and the 802.1p priority of the data traffic packet is 1.

53.3.2 Configure Remarking *-B -S -E -A*

Network Requirements

- There are two servers in the network, that is, Video server and Data server.
- Configure the remarking function, realizing that the 802.1p priority of the video traffic packet is marked as 5 and the 802.1p priority of the data traffic packet does not change.

Network Topology

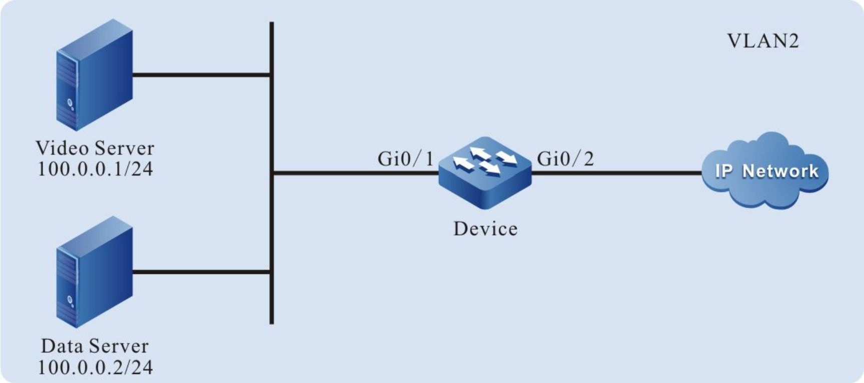


Figure 53-3 Networking of configuring the remarking

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 as Trunk and permit the services of VLAN2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the L3 action group.

#Configure the L3 action group named remark and the action is to remark the 802.1p priority of the packet as 5.

```
Device(config)#l3-action-group remark
Device(config-action-group)#remark l2-priority dot1p 5
Device(config-action-group)#exit
```

Step 3: Configure the IP standard ACL.

#Configure the IP standard ACL with serial number 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding the rule with the L3 action group named remark, realizing that the 802.1p priority of the video traffic packet is remarked as 5.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group remark
```

#Configure the rule, permitting the data traffic to pass and not modifying the 802.1p priority of the packet.

```
Device(config-std-nacl)#permit host 100.0.0.2
Device(config-std-nacl)#exit
```

Step 4: Configure applying the IP standard ACL.

#Apply the IP standard ACL with serial number 1 to the ingress direction of port gigabitethernet0/1 on Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1                    IN           IP         1
```

Step 5: Check the result.

#After the video traffic and data traffic are processed by Device, the 802.1p priority of the video traffic packet sent out from port gigabitethernet0/2 is modified to 5 and the 802.1p priority of the data traffic packet does not change.

53.3.3 Configure Traffic Shaping *-B -S -E -A*

Network Requirements

- There are two servers in the network, that is, Video server and Data server.
- Configure the traffic shaping function; ensure that the video traffic rate is 20000kbps, but cannot exceed 20000kbps; the total of the video traffic rate and the data traffic rate does not exceed 50000kbps. When the video traffic rate is larger than 20000kbps, limit the video traffic rate as 20000kbps; when the video traffic rate is smaller than 20000kbps, the remaining bandwidth is occupied by the data traffic.

Network Topology

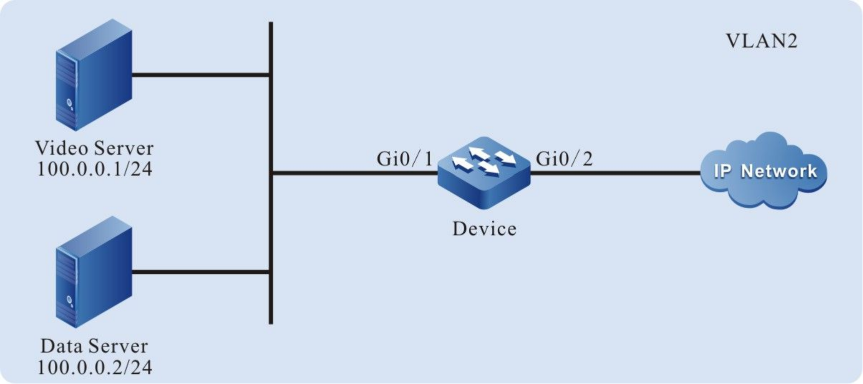


Figure 53-4 Networking of configuring the traffic shaping

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 as Trunk and permit the services of VLAN2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the L3 action group.

#Configure the L3 action group named LP7 and the action is to remark the packet to queue 7.

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#Configure the L3 action group named LP6 and the action is to remark the packet to queue 6.

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

Step 3: Configure the IP standard ACL.

#Configure the IP standard ACL with serial number 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding the rule with the L3 action group named LP7, realizing that the video traffic packet is remarked to queue 7.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#Configure binding the rule with the L3 action group named LP6, realizing that the video traffic packet is remarked to queue 6.

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
Device(config-std-nacl)#exit
```

Step 4: Configure applying the IP standard ACL.

#Apply the IP standard ACL with serial number 1 to the ingress direction of port gigabitethernet0/1 on Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1                    IN           IP         1
```

Step 5: Configure the traffic shaping function.

#Configure the queue-based traffic shaping on port gigabitethernet0/2 and limit the rate of the traffic in queue 7 to 20000kbps.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#traffic-shape queue 7 20000 4096 20000 4096
```

#Configure the port-based traffic shaping on port gigabitethernet0/2 and limit the rate of the port traffic to 50000kbps.

```
Device(config-if-gigabitethernet0/2)#traffic-shape 50000 4096
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#After the video traffic and data traffic are processed by Device, the total of the video traffic rate and the data traffic rate sent out from port gigabitethernet0/2 does not exceed 50000kbps. When the video traffic rate is larger than 20000kbps, limit the video traffic rate as 20000kbps; when the video traffic rate is smaller than 20000kbps, the remaining bandwidth can be occupied by the data traffic.

53.3.4 Configure Rate Limitation *-B -S -E -A*

Network Requirements

- There are two servers in the network, that is, Video server and Data server.
- Configure the rate limitation function, and limit the total of the video traffic rate and the data traffic rate not to exceed 50000kbps. The data traffic rate does not exceed 20000kbps.

Network Topology

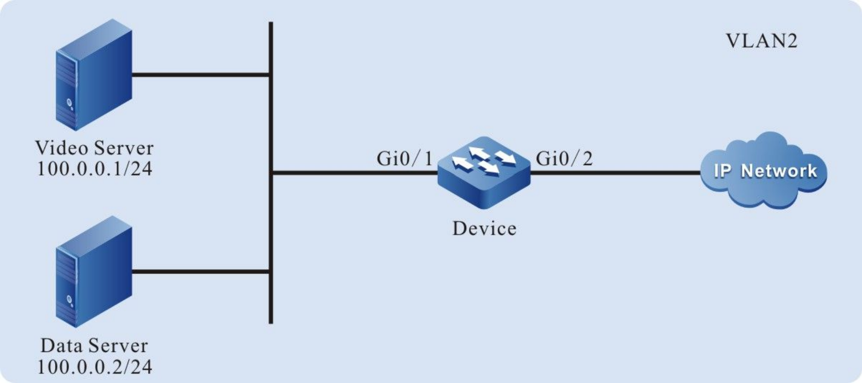


Figure 53-5 Networking of configuring the rate limitation

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 as Trunk and permit the services of VLAN2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the rate limitation function.

#Configure the port-based rate limitation on port gigabitethernet0/1 and limit the traffic rate to 50000kbps.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#rate-limit default 50000 4096
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Configure the meter function.

#Configure the meter named data_stream and limit the traffic rate to 20000kbps.

```
Device(config)#traffic-meter data_stream
Device(config-meter)#meter mode srtcm 20000 4096 4096
Device(config-meter)#exit
```

Step 4: Configure the egress action group.

#Configure the egress action group named data_stream and apply the meter in the egress action group.

```
Device(config)#egr-action-group data_stream
Device(config-egract-group)#meter data_stream
Device(config-egract-group)#exit
```

Step 5: Configure the IP standard ACL.

#Configure the IP standard ACL with serial number 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding the rule with the egress action group named data_stream, and limit the data traffic rate to 20000kbps.

```
Device(config-std-nacl)#permit host 100.0.0.2 egr-action-group data_stream
```

#Configure the rule and permit the video traffic to pass.

```
Device(config-std-nacl)#permit host 100.0.0.1
Device(config-std-nacl)#exit
```

Step 6: Configure applying the IP standard ACL.

#Apply the IP standard ACL with serial number 1 to the egress direction of port gigabitethernet0/2 on Device.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#ip access-group 1 out
Device(config-if-gigabitethernet0/2)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/2                    OUT           IP         1
```

Step 7: Check the result.

#After the video traffic and data traffic are processed by Device, the total of the video traffic rate and the data traffic sent out from port gigabitethernet0/2 does not exceed 50000kbps and the data traffic rate does not exceed 20000kbps.

53.3.5 Configure WRED *-B -S -E -A*

Network Requirements

- Lots of terminals download files from the FTP server.
- Configure the WRED function on Device, preventing the TCP global synchronization from resulting in the intermittent FTP connection.

Network Topology

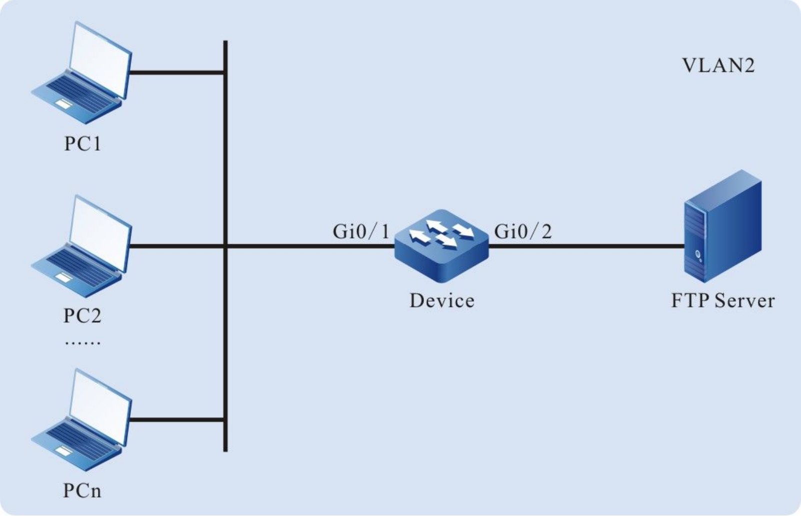


Figure 53-6 Networking of configuring WRED

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 as Trunk and permit the services of VLAN2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the WRED function.

#Configure the drop start value of the packet in queue 0 on port gigabitethernet0/2 as 80 and the drop rate as 45.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#drop-mode 0 wred drop-start 80 drop-rate 45 Device(config-
if-gigabitethernet0/2)#exit
```

NOTE

- The packets sent from PC are all Untag packets and enter queue 0 by default.

Step 3: Check the result.

#When lots of terminals download files from the FTP server, the intermittent FTP connection does not happen.

53.3.6 Configure SP *-B -S -E -A*

Network Requirements

- There is authentication server (AAA Server), video server and one terminal device (PC) in the network.
- Configure the SP function. When the traffic of the egress port is congested, first ensure the traffic of the authentication server, then the video traffic, and at last, the terminal traffic.

Network Topology

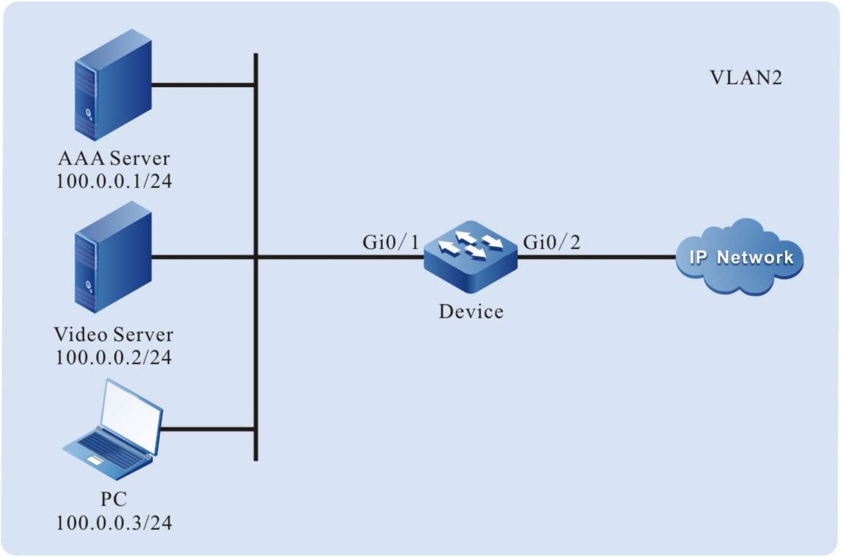


Figure 53-7 Networking of configuring the SP

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 as Trunk and permit the services of VLAN2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the L3 action group.

#Configure the L3 action group named LP7 and the action is to remark the packets to queue 7.

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#Configure the L3 action group named LP6 and the action is to remark the packets to queue 6.

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

#Configure the L3 action group named LP5 and the action is to remark the packets to queue 5.

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority 1p 5
Device(config-action-group)#exit
```

Step 3: Configure the IP standard ACL.

#Configure the IP standard ACL with serial number 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding the rule with the L3 action group named LP7, realizing that the authentication traffic packets are remarked to queue 7.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#Configure binding the rule with the L3 action group named LP6, realizing that the authentication traffic packets are remarked to queue 6.

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#Configure binding the rule with the L3 action group named LP5, realizing that the authentication traffic packets are remarked to queue 5.

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
Device(config-std-nacl)#exit
```

Step 4: Configure applying the IP standard ACL.

#Apply the IP standard ACL with serial number 1 to the ingress direction of port gigabitethernet0/1 on Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface---------------Direction----AclType----AclName
gi0/1                   IN           IP         1
```

Step 5: Configure the SP function.

#Configure the SP function on port gigabitethernet0/2 and perform the strict priority scheduling for the packet.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule sp
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#When the traffic of the egress port gigabitethernet0/2 is congested, first permit the authentication traffic to pass, then video traffic, and at last, the terminal traffic.

53.3.7 Configure WDRR *-B -S -E -A*

Network Requirements

- There is authentication server (AAA Server), video server and one terminal device (PC) in the network.
- Configure the WDRR function. When the traffic of the egress port is congested, realize that the terminal traffic, video traffic and authentication traffic pass by some specified proportion.

Network Topology

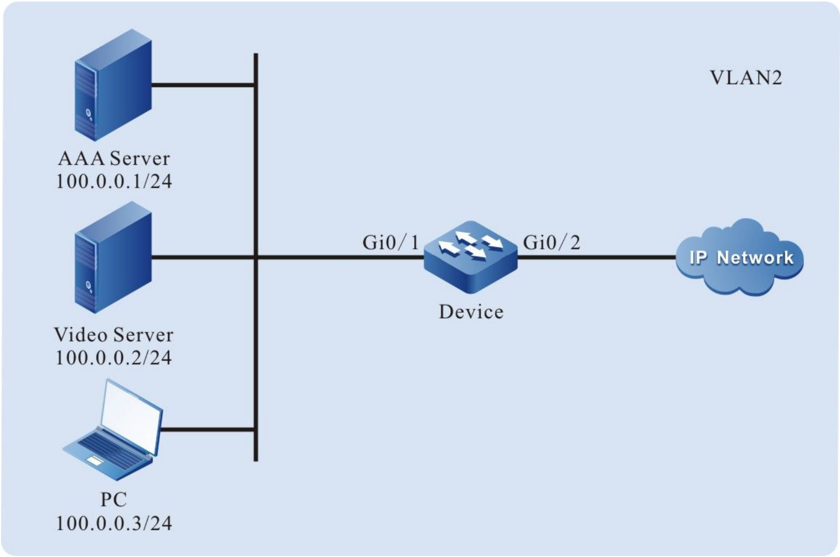


Figure 53-8 Networking of configuring the WDRR

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 as Trunk and permit the services of VLAN2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the L3 action group.

#Configure the L3 action group named LP7 and the action is to remark the packet to queue 7.

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#Configure the L3 action group named LP6 and the action is to remark the packet to queue 6.

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

#Configure the L3 action group named LP5 and the action is to remark the packet to queue 5.

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority 1p 5
Device(config-action-group)#exit
```

Step 3: Configure the IP standard ACL.

#Configure the IP standard ACL with serial number 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding the rule with the L3 action group named LP7, realizing that the authentication traffic packets are remarked to queue 7.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#Configure binding the rule with the L3 action group named LP6, realizing that the authentication traffic packets are remarked to queue 6.

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#Configure binding the rule with the L3 action group named LP5, realizing that the authentication traffic packets are remarked to queue 5.

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
Device(config-std-nacl)#exit
```

Step 4: Configure applying the IP standard ACL.

#Apply the IP standard ACL with serial number 1 to the ingress direction of port gigabitethernet0/1 on Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1                    IN           IP         1
```

Step 5: Configure the WDRR function.

#Configure the WDRR function on port gigabitethernet0/2, scheduling the packets of queue 5, queue 6 and queue 7 by the proportion of 1:2:3.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule wdrr 1 1 1 1 1 1 2 3
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#When the traffic of the egress port gigabitethernet0/2 is congested and the packet bytes are consistent, the terminal traffic, video traffic and authentication traffic pass by the proportion of 1:2:3; when the packet bytes are not consistent, the terminal traffic, video traffic and authentication traffic pass by the proportion of (1*the bytes of the authentication packet): (2*the bytes of the video bytes):(3*the bytes of the terminal packet).

53.3.8 Configure SP+WRR *-B -S -E -A*

Network Requirements

- There is authentication server (AAA Server), video server and one terminal device (PC) in the network.
- Configure the SP+WRR function. When the traffic of the egress port is congested, first ensure that the traffic of the authentication server all can pass and the terminal traffic and video traffic can pass by the proportion of 1:2.

Network Topology

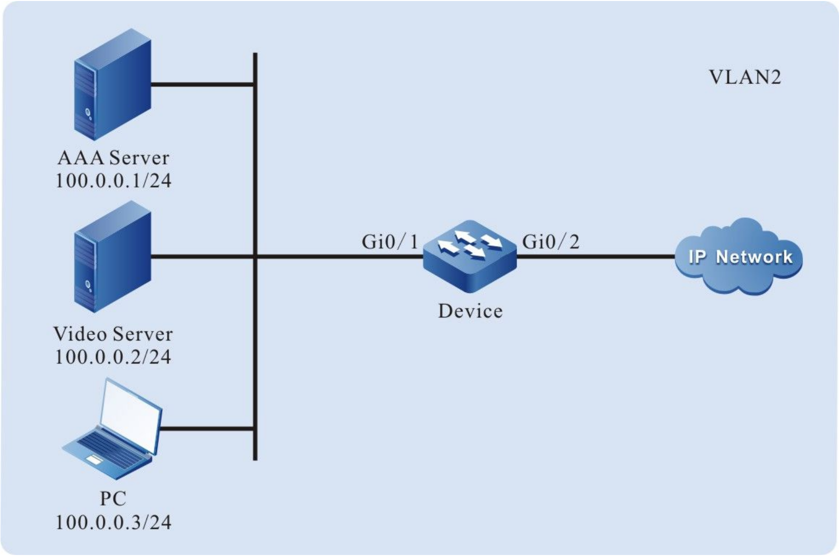


Figure 53-9Networking of configuring the SP+WRR

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#Configure the link type of port gigabitethernet0/2 as Trunk and permit the services of VLAN2 to pass.

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the L3 action group.

#Configure the L3 action group named LP7 and the action is to remark the packet to queue 7.

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority lp 7
Device(config-action-group)#exit
```

#Configure the L3 action group named LP6 and the action is to remark the packet to queue 6.

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority lp 6
Device(config-action-group)#exit
```

#Configure the L3 action group named LP5 and the action is to remark the packet to queue 5.

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority lp 5
Device(config-action-group)#exit
```

Step 3: Configure the IP standard ACL.

#Configure the IP standard ACL with serial number 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding the rule with the L3 action group named LP7, realizing that the authentication traffic packets are remarked to queue 7.

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#Configure binding the rule with the L3 action group named LP6, realizing that the authentication traffic packets are remarked to queue 6.

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#Configure binding the rule with the L3 action group named LP5, realizing that the authentication traffic packets are remarked to queue 5.

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
Device(config-std-nacl)#exit
```

Step 4: Configure applying the IP standard ACL..

#Apply the IP standard ACL with serial number 1 to the ingress direction of port gigabitethernet0/1 on Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1                    IN           IP         1
```

Step 5: Configure the SP + WRR function.

#Configure the SP+WRR function on port gigabitethernet0/2, permitting all the packets of queue 7 to pass and scheduling the packets of queue 5 and queue 6 by the proportion of 1:2.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule wrr 1 1 1 1 1 1 2 0
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#When the traffic of port gigabitethernet0/2 is congested, the authentication traffic all passes first. The terminal traffic and video traffic pass by the proportion of 1:2.

53.3.9 Configure Flow Mirror *-B -S -E -A*

Network Requirements

- PC1, PC2 and PC3 are connected with Device; PC1 and PC2 communicate in VLAN2.
- Configure the flow mirror function on Device, realizing that PC3 monitor the packets received by port gigabitethernet0/1 of Device.

Network Topology

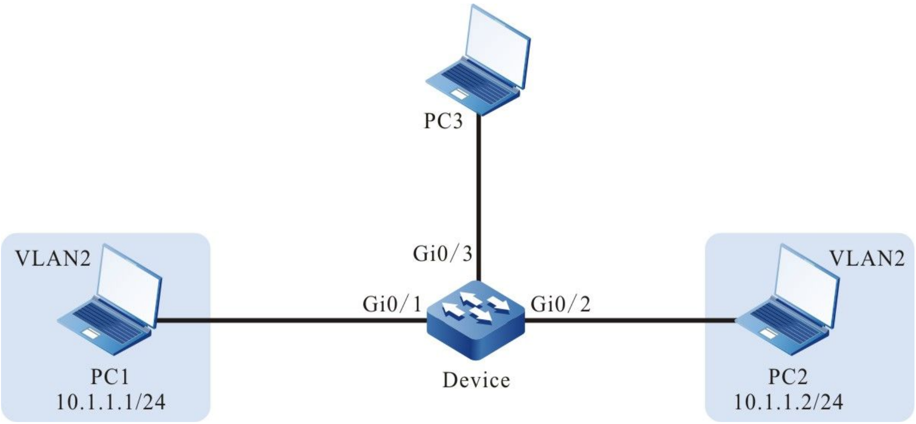


Figure 53-10 Networking of configuring the flow mirror

Configuration Steps

Step 1: Configure the link type of the VLAN and port.

#Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device as Access and permit the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the flow mirror function.

#Configure the L3 action group named mirror and mirror the packet to port gigabitethernet0/3.

```
Device(config)#l3-action-group mirror
Device(config-action-group)#mirror interface gigabitethernet 0/3
Device(config-action-group)#exit
```

Step 3: Configure the counter function.

#Configure the egress action group named count, counting the number of the packets.

```
Device(config)#egr-action-group count
Device(config-egract-group)#count all-colors
Device(config-egract-group)#exit
```

Step 4: Configure the IP standard ACL.

#Configure the IP standard ACL with serial number 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure binding the rule with the L3 action group named mirror, realizing that all packets are mirrored to port gigabitethernet0/3.

```
Device(config-std-nacl)#permit any l3-action-group mirror
Device(config-std-nacl)#exit
```

#Configure the IP standard ACL with serial number 2 on Device.

```
Device(config)#ip access-list standard 2
```

#Configure binding the rule with the egress action group named count, counting all packets.

```
Device(config-std-nacl)#permit any egr-action-group count
Device(config-std-nacl)#exit
```

Step 5: Configure applying the IP standard ACL..

#Apply the IP standard ACL with serial number 1 to the ingress direction of port gigabitethernet0/1 on Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#Apply the IP standard ACL with serial number 2 to the egress direction of port gigabitethernet0/3 on Device.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#ip access-group 2 out
Device(config-if-gigabitethernet0/3)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1                    IN           IP         1
gi0/3                    OUT          IP         2
```

Step 6: Check the result.

#When PC1 and PC2 communicate with each other, we can capture the packets received by port gigabitethernet0/1 on PC3.

#View the number of the packets measured by the counter on Device.

```
Device#show traffic-count inst-interface gigabitethernet 0/3 ip-out
Interface              Instance_type                Acl_name
gigabitethernet0/3     Ip Acl Bind Interface Out    2
--------------------------------------------------------------------
seq                    :                            10
counter_mode           :                            count all color
all packets number     :                            5
all packets byte       :                            640
```

We can see that there are five packets measured at the egress direction of port gigabitethernet0/3.

54 CPU Protection

54.1 Overview

There are lots of protocol packets in the device that need to be sent to CPU for processing and we need to specify the queue for each kind of protocol packets. The CPU protection function classifies the protocol packets sent to CPU and the packets enter different CPU queues according to the different protocol priorities. We can set the rate limitation of each queue.

The device totally has eight queues, numbering from 0 to 7. They adopt the strict priorities. The smaller the number is, the lower the priority is. That is to say, the priority of queue 0 is the lowest and the priority of queue 7 is the highest. The packets in the queue with the high priority are earlier sent to the CPU for processing that the packets in the queue with low priority. We can specify them to different priorities of queues according to the importance of each kind of packets, ensuring that the important packets are first sent to the CPU for processing.

Meanwhile, the device can perform the rate limitation for the packets entering each CPU queue, preventing the vicious protocol packet attack in the network from causing the too high CPU utilization of the device and resulting in the abnormal running of the device.

54.2 CPU Protection Function Configuration

Table 54-1 The Configuration List of the CPU Protection Function

Configuration Task	
Configure the CPU queue of the protocol packet	Configure the CPU queue of the protocol packet
Configure the rate limitation of the CPU queue	Configure the rate limitation of the CPU queue
Configure the route protocol packet to be processed by CPU	Enable the unicast route protocol packet to be processed by CPU
	Enable the multicast route protocol packet to be processed by CPU
Configure the customized protocol packet to be processed by CPU	Configure the matching rule of the customized protocol packet to be processed by CPU

Configuration Task	
	Configure the mode of the customized protocol packet to be processed by CPU

54.2.1 Configure CPU Queue of Protocol Packets *-B -S -E -A*

Configuration Conditions

None

Configure CPU Queue of Protocol Packets

The device totally has eight queues and the user can configure different protocol packets to enter different queues. The device sends the protocol packets to the CPU for processing in order from high priority queue to low priority queue according to the user configuration. If the protocol packets are in the queue with high priority, they first get the CPU processing. Besides, the user also can specify the important packet to enter the high priority queue, ensuring that the important packets are first sent to the CPU for processing. By default, different protocol packets enter the default CPU queue. Besides, we also can use the command to modify the packet to enter the specified CPU queue.

Table 54-2 Configure CPU Queue of Protocol Packets

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the CPU queue the protocol packets enter	**cpu-packet** *protocol* **cos** *cos-value*	Mandatory By default, different protocol packets enter the default CPU queue.

54.2.2 Configure Line Rate(LR) for All CPU Queues *-B -S -E -A*

Configuration Conditions

None

Configure Line Rate(LR) for All CPU Queues

In order to prevent malicious attacks from causing excessively high CPU utilization that makes the Device unable to run, the user may configure a line rate(LR) for all CPU queues. In case the overall message rate of all queues exceeds this LR as a result of malicious attacks, the message will be discarded in order to prevent CPU utilization from going even higher.

Table 54-3 Configure Line Rate(LR) for All CPU Queues

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure line rate(LR) for all CPU queues	**cpu-packet cos global pps** *pps-value*	Required By default, LR for all queues is 2000PPS

54.2.3 Configure Rate Limitation of CPU Queue *-B -S -E -A*

Configuration Conditions

None

Configure Rate Limitation of CPU Queue

To prevent the vicious attack in the network from causing the too high CPU utilization and the device cannot run, the user can configure the rate limitation of each CPU queue. If there is attack and the packet rate in the queue exceeds the limited rate of the queue, the packet is dropped, avoiding causing the too high CPU utilization. By default, different CPU queues set different limited rates. The user can modify the limited rate of the CPU queue as desired.

Table 54-4 Configure Rate Limitation of CPU Queue

Step	**Command**	**Description**
Enter global configuration mode	**configure terminal**	-
Configure the rate limitation of the CPU queue	**cpu-packet cos** *cos-value* **pps** *pps-value*	Mandatory By default, the rate limitation of each queue is different.

54.2.4 Configure Customized Protocol Packet to Be Processed by CPU *-B -S -E -A*

Configuration Conditions

None

Configure Matching Rule of Customized Protocol Packet to Be Processed by CPU

The configured matching rule of the customized protocol packet to be processed by CPU should be used with the mode of the customized protocol packet to be processed by CPU. It performs the corresponding action processing for the packet meeting the match rule. The match rule includes dst-mac (destination MAC address), ingress (interface), vlan-id (VLAN ID), ether-type (Ethernet type), IP (IPV4), IPV6, 0x0000 (customized Ethernet type), ip-protocol (IP protocol, such as IGMP and TCP), dst-ip (destination IP), src-port (source port), and dst-port. The user can combine the above match rules to use as desired.

Table 54-5 Configure the Match Rule of the Customized Protocol Packet to Be Processed by CPU

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the match rule of the customized protocol	**cpu-packet user-define** *user-id* **match** { **dst-mac** *dst-mac* | **ether-type** { *ether-type-value* | **ip** [**dst-ip** *dst-ip-address* | **dst-mac** *dst-mac* | **ingress** *ingress-interface* | **ip-known-unicast** | **ip-protocol** *protocol-type* | **vlan-id** *vlan-id* [**dst-ip** *dst-ip-address* | **ingress** *ingress-interface* | **ip-known-unicast** | **ip-protocol** *protocol-type*]] | **ipv6** [**dst-ip6** *dst-ipv6-address* | **dst-mac** *dst-mac* | **ingress** *ingress-interface* | **ip-known-unicast** | **ip-protocol** *protocol-type* | **vlan-id** *vlan-id* [**dst-ip** *dst-ip-address* | **ingress** *ingress-interface* | **ip-known-unicast** | **ip-protocol** *protocol-type*]] } | **ingress** *ingress-interface* | **vlan-id** *vlan-id* [**ingress** *ingress-interface*] }	Mandatory By default, there is no any match rule.

Configure Mode of Customized Protocol Packet to Be Processed by CPU

The configured matching rule of the customized protocol packet to be processed by CPU should be used with the mode of the customized protocol packet to be processed by CPU. It performs the corresponding action processing for the packet meeting the match rule. For example, if the configured mode is copy, do not change the original forwarding process of the packet, but copy the packet to CPU for processing; if the configured mode is drop, do not permit to send the packet to CPU for processing, but drop the packet; if the configured mode is remark, modify the priority of the packet to be processed by CPU; if the configured mode is trap, change the original forwarding process of the packet by only sending the packet to CPU for processing instead of forwarding the packet.

Table 54-6 Configure the Mode of Sending the Customized Protocol Packet to CPU

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the action of the customized protocol packet to be processed by CPU	**cpu-packet user-define** *user-id* **action** { **drop** | { **copy** | **remark** | **trap** } **cos** *cos-value* }	Mandatory By default, do not perform any action for the packet meeting the match rule. When the processing modes of the customized protocol packet by CPU are copy, remark and trap, you can specify the COS value.

54.2.5 Monitoring and Maintaining of CPU Protection *-B -S -E -A*

Table 54-7 Monitoring and Maintaining of the CPU Protection

Command	Description
show cpu-packet acl-table	Display all information delivered by the CPU protection to ACL entries
show cpu-packet cos	Display the current and default queue information of the protocol packets to be processed by CPU
show cpu-packet mac-table	Display the MAC entry information delivered via the CPU protection

Command	Description
show cpu-packet port-table	Display the port-based BroadShield entry information delivered via the CPU protection
show cpu-packet pps	Display the rate limitation information of each CPU queue
show cpu-packet switch-table	Display the global BroadShield entry information based on the whole device delivered via the CPU protection
show cpu-packet udf-table	Display all customized ACL entry information set via the CPU protection module

54.3 Typical Configuration Example of CPU Protection

54.3.1 Configure Basic Functions of CPU Protection *-B -S -E -A*

Network Requirements

- PC is connected to IP Network via Device.
- Configure the SVI-IP packet to queue 5 on Device so that the SVI-IP packets of the device can first get the CPU processing.
- Perform the rate limitation for the queue of ARP on Device so that when the CPU utilization of Device is too high, the packet with low priority can be processed normally.

Network Topology

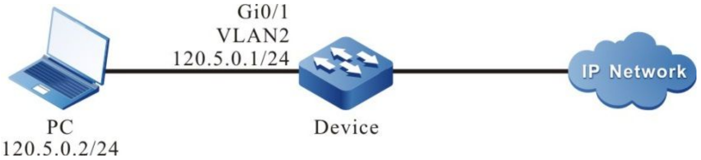


Figure 54–1 Networking of Configuring the CPU Protection Basic Functions

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the CPU queue of the SVI-IP packet.

# Configure the SVI-IP packet to queue 5 on Device.

```
Device#configure terminal
Device(config)#cpu-packet svi-ip cos 5
```

Step 4: Configure the rate limitation of the CPU queue.

# Configure the limited rate of the CPU queue on Device as 50pps.

```
Device#configure terminal
Device(config)#cpu-packet cos 1 pps 50
```

Step 5: Check the result.

#View the CPU queue of the protocol packets on Device.

```
Device#show cpu-packet cos
Type                    Current-CoS    [Default-CoS]
------------------------------------------------------
random                   0              [0]
lookup-miss              0              [0]
ipv6-all                 0              [0]
udp-broadcast            0              [0]
icmp                     0              [0]
ip-e-packet              0              [0]
ip                       0              [0]
mpls-unicast             0              [0]
mpls-multicast           0              [0]
arp                      1              [1]
ip6-solicited-node       1              [1]
host-group               1              [1]
router-group             1              [1]
lldp                     2              [2]
dot1x                    2              [2]
dhcp                     2              [2]
pim                      3              [3]
igmp-dvmrp               3              [3]
ip4-reserved-multicast   3              [3]
ip6-reserved-multicast   3              [3]
ip6-interface-multicast  3              [3]
esp                      4              [4]
ah                       4              [4]
irmp                     4              [4]
rip                      4              [4]
is-is                    4              [4]
bgp                      4              [4]
ldp                      4              [4]
rsvp                     4              [4]
ospf                     4              [4]
gvrp                     5              [5]
l2pt                     5              [5]
ethernet-cfm             5              [5]
ethernet-lmi             5              [5]
l2-interface-unicast     5              [5]
cmp                      5              [5]
ndsp-ulfd                5              [5]
svi-ip                   5              [2]
loopback-detect          6              [6]
stp-bpdu                 6              [6]
slow-protocols           6              [6]
telnet-ssh               6              [6]
radius                   6              [6]
vbrp                     6              [6]
vrrp                     6              [6]
bfd                      6              [6]
eips                     7              [7]
```

```
ulpp                    7              [7]
```

You can see that the CPU queue of SVI-IP on Device is adjusted from the default queue 2 to queue 5.

#View the rate limitation of the queue on Device.

```
Device#show cpu-packet pps
CoS   Current-PPS   [Default-PPS]
---------------------------------
0     200           [200]
1     50            [250]
2     500           [500]
3     600           [600]
4     1000          [1000]
5     400           [400]
6     300           [300]
7     100           [100]
```

You can see that the limited rate of queue 1 of ARP on device is modified from the default 250pps to 50pps.

54.3.2 Configure Customized Rule of CPU Protection *-B -S -E -A*

Network Requirements

- Device is directly connected to PC1 and PC2.
- Configure the customized rule of the CPU protection on Device and trap the packet matching the condition to CPU for processing and enter the corresponding queue.

Network Topology

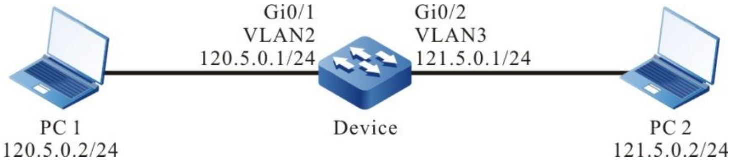


Figure 54–2 Networking of Configuring the Customized Rule of the CPU Protection

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the customized rule of the CPU protection.

#Configure the customized rule and trap the IP packet with destination address 121.5.0.2 to CPU for processing, and set the COS value as 5.

```
Device#configure terminal
Device(config)#cpu-packet user-define 1 match ether-type ip dst-ip host 121.5.0.2
Device(config)#cpu-packet user-define 1 action trap cos 5
```

Step 4: Check the result.

#View the customized rule on Device.

```
Device#show cpu-packet udf-table
user-define 1
 ether-type: 0x0800(IPv4)
 dst-ip: host 121.5.0.2
 location: global
 valid: yes
 action: trap
 CoS: 5
```

#When PC1 accesses PC2, the customized rule of the CPU rule takes effect and trap the IP packet with destination address 121.5.0.2 on Device to CPU for processing and enter queue 5.

NOTE

- When the customized rule matches other condition and executes other modes, refer to the configuration.

55 Port Security

55.1 Overview

55.1.1 Overview of Port Security *-B -S -E -A*

Port security is the security mechanism of controlling the devices connected to the network. It is applied to the access layer and can limit the hosts of using the device port, permitting some specified hosts to access the network, while the other hosts cannot access the network.

The port security function can bind the user MAC address, IP address, VLAN ID and port number, preventing the invalid user from accessing the network, so as to ensure the security of the network data and the valid user can get the enough bandwidth.

55.1.2 Port Security Rule *-B -S -E -A*

The port security rule is divided to four kinds:

MAC rule: Control whether the host can communicate according to the MAC address of the host. The binding mode of the MAC rule contains MAC binding, MAC+VLAN binding, and MAC+IP binding.

IP rule: Control whether the host can communicate according to the IP address of the host. The IP rule can be for the binding of a single IP address and also can be for the binding of the IP address segment.

MAX rule: Limit the number of the MAC addresses that can be learned by the port freely to control the host communication. The number of the MAC address entries does not contain the valid MAC address entries generated by the MAC rule and IP rule.

STICKY rule: Control whether the host can communicate according to the MAC address of the host. The binding mode of the STICKY rule contains the MAC binding and MAC+VLAN binding. The STICKY rule can automatically learn and also can configure manually, and is saved in the running configuration. If saving the running configuration before the device restarts, do not need to configure again after the device restarts and the STICKY rule automatically takes effect. When enabling the STICKY function in the port, convert the dynamic MAC entry learned by the MAX rule to the STICKY rule and save in the running configuration.

55.1.3 Work Principle of Port Security *-B -S -E -A*

If only enabling the port security, the port security drops all packets received on the port. The rules of the port security rely on the ARP packets and IP packets of the device to trigger. When the device receives the ARP packet and IP packet, the port security extracts various packet information and matches with the configured rule. The matching order is first match the MAC rule, secondly match the STICKY rule, then match the IP rule and at last match the MAX rule, and control the L2 forwarding table of the port according to the matching result, so as to control the forwarding action of the port for the packet. The valid packet matching the MAX rule or STICKY rule is forwarded. For the packet matching the MAC rule or IP rule, if the action of the rule for the packet is permit, the packet belongs to the valid packet and is forwarded. Otherwise, the packet is invalid and dropped.

The action is the permitted MAC rule and IP rule. After taking effect, write the MAC address of the rule to the L2 forwarding table so that the L2 forwarding can be performed for the packets matching the rule. If the action is the refused Mac rule and IP rule, the corresponding MAC is not written to the L2 forwarding table and the packet needs to be dropped via the port security.

After MAC rule and STICKY rule take effect, write to the MAC address entries to form the effective entries, making the packet perform the L2 forwarding.

55.2 Port Security Function Configuration

Table 55-1 Basic Function Configuration List of the Port Security

Configuration Task	
Configure the basic functions of the port security	Enable the port security function
Configure the port security rule	Configure the MAC rule
	Configure the IP rule
	Configure the MAX rule
	Configure the STICKY rule
Configure the aging function of the static MAC address	Enable the aging function of the static MAC address
	Configure the age time of the static MAC address
Configure the processing mode when receiving the invalid packet	Configure the processing mode when receiving the invalid packet
Configure the log sending interval when receiving the invalid packet	Configure the log sending interval when receiving the invalid packet

55.2.1 Configure Basic Functions of Port Security *-B -S -E -A*

In the configuration tasks of the port security, you should first enable the port security so that the configuration of the other functions can take effect.

Configuration Conditions

None

Enable Port Security Function

After enabling the port security and if not configuring any port security rule, the port cannot learn the MAC address.

Table 55-2 Configure the Basic Functions of the Port Security

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the port security function	**port-security enable**	Mandatory By default, the port security function is not enabled.

NOTE

- The port security and 802.1x cannot be used on one port at the same time.
- The port security and MAC address authentication cannot be used on one port at the same time.
- The port security and DAI (Dynamic ARP Inspection) cannot be used on one port at the same time.

55.2.2 Configure Port Security Rule *-B -S -E -A*

Configuration Conditions

Before configuring the port security rule, first complete the following task:

- Enable the port security function

Configure MAC Rule

If hoping to control whether the terminal can communicate via the MAC address, the user can use the MAC rule and the packets whose matching action is permit rule can be forwarded. The packets whose matching action is refuse rule are dropped.

Table 55-3 Configure MAC Rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the MAC rule whose action is permit	**port-security permit mac-address** *mac-address-value* [**desc** *security-rule-description* **|** **ip-address** *ip-address-value* [**desc** *security-rule-description*] **| vlan-id** *vlan-id* [**desc** *security-rule-description*]]	Either By default, the MAC rule is not configured in the port.
Configure the MAC rule whose action is refuse	**port-security deny mac-address** *mac-address-value* [**ip-address** *ip-address-value* **| vlan-id** *vlan-id*]	

Configure IP Rule

If hoping to control whether the terminal can communicate via the IP address, the user can use the IP rule and the packets whose matching action is the permit rule can be forwarded. The packets whose matching action is the refuse rule are dropped.

Table 55-4 Configure IP Rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the IP rule whose action is permit	**port-security permit ip-address** *ip-address-value* [**to** *ip-address-value*]	Either By default, the IP rule is not configured in the port.
Configure the IP rule whose action is refuse	**port-security deny ip-address** *ip-address-value* [**to** *ip-address-value*]	

Configure MAX Rule

In the port enabled with the port security function, if hoping that the connected terminal not matching the MAC rule or IP rule also can communicate, the user can configure the MAX rule, the rule limits the number of the permitted access terminals.

Table 55-5 Configure MAX Rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure the MAX rule	**port-security maximum** *maximum-number*	Mandatory By default, the number of the MAC addresses permitted to be learned by the MAX rule is 0.

NOTE

- The number of the dynamic addresses actually learned by the MAX rule is limited by the port, VLAN and the number of the system MAC addresses.

Configure STICKY Rule

If hoping that the MAC address and the VLAN information of the terminal permitted by the MAX rule can be saved in the configuration, the user can enable the STICKY function on the device so that the entries learned by the device via the MAX rule can be converted to the STICKY rule. After converting, the user can adjust the MAX rule quantity via the number of the current STICKY rules so that only the terminals matching the STICKY rule can communicate. In this way, the device can automatically learn the MAC address of the access terminal, convert to the STICKY rule, and save in the configuration, avoiding the operation of configuring the MAC rule manually.

Table 55-6 Configure STICKY Rule

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		just takes effect on the aggregation group.
Configure the MAX rule	**port-security maximum** *maximum-number*	Mandatory By default, the number of the dynamic MAC addresses permitted to be learned by the MAX rule is 0. The STICKY rule can be configured only after configuring the number of the MAX rules.
Enable the STICKY function	**port-security permit mac-address sticky**	Mandatory By default, the STICKY function is disabled. The STICKY rule can be configured only after enabling the STICKY function.
Configure the STICKY rule	**port-security permit mac-address sticky** [*mac-address-value* [**desc** *security-rule-description* | **vlan-id** *vlan-id* [**desc** *security-rule-description*]]]	Mandatory By default, the STICKY rule is not configured in the port.

55.2.3 Configure STICKY Rule Learning Mode *-B -S -E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of STICKY rules learning mode:

- Enable port security function.

Configure STICKY Rule Learning Mode

If the user wishes to conduct STICKY learning in MAC or MAC+VLAN mode, he/she can set the STICKY rule learning mode to MAC; if the user wants to perform STICKY rule learning in MAC+IP mode, he/she can set the STICKY rule learning mode to MAC+IP.

Table 2-7 Configure STICKY Rule Learning Mode

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2 ethernet interface configuration mode	**interface** *interface-name*	Must be chosen alternatively After entering L2 ethernet interface configuration mode, subsequent configurations only apply to current port; in aggregation group configuration mode, subsequent configurations only take effect in aggregation group
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure STICKY rule learning mode	**port-security permit mac-address sticky mode** { **mac** | **mac-ip** }	Required By default, the STICKY rule learning mode is MAC mode

55.2.4 Configure Aging Function of Static MAC Address *-B -S -E -A*

Configuration Conditions

Before configuring the aging function of the static MAC address, first complete the following task:

- Enable the port security function

Enable Aging Function of Static MAC Address

To detect whether the terminal of the effective entry of the MAC rule or IP rule is online, the user can enable the aging function of the static MAC address. After the aging function of the static MAC address and if it is detected that the terminal is offline, the effective entry of the terminal is deleted so that the chip resources can be released.

Table 55-8 Enable Aging Function of Static MAC Address

Step	**Command**	**Description**
Enter global configuration mode	**configure terminal**	-

Step	Command	Description
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the aging function of the static MAC address	**port-security aging static**	Mandatory By default, the aging function of the static MAC address is disabled.

Configure Age Time of Static MAC Address

The user can configure the reasonable age time according to the actual network environment configuration. In the general application, just keep the default value.

Table 55-9 Configure Age Time of Static MAC Address

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the age time of the static MAC address	**port-security aging time** *time-value*	Mandatory

Step	Command	Description
		By default, the age time of the static MAC address is 1 minute.

55.2.5 Configure Processing Mode when Receiving Invalid Packet *-B -S -E -A*

Configuration Conditions

Before configuring the processing mode when receiving the invalid packet, first complete the following task:

- Enable the port security function

Configure Processing Mode when Receiving Invalid Packet

The port security provides three kinds of processing modes for the invalid packet, that is, protect, restrict and shutdown. The user can select according to the security requirement. The specific functions of the three processing modes are as follows:

- **protect**: After receiving the invalid packet, drop the packet.
- **restrict**: After receiving the invalid packet, drop the packet and trap the information to the NMS.
- **shutdown**: After receiving the invalid packet, drop the packet, disable the port receiving the packet and trap the information to the NMS.

Table 55-10 Configure Processing Mode when Receiving Invalid Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the processing mode of the invalid packet	**port-security violation** { **protect** | **restrict** | **shutdown** }	Mandatory By default, the processing mode when the port security receives the invalid packet is **protect**.

55.2.6 Configure Log Sending Interval when Receiving Invalid Packet

-B -S -E -A

Configuration Conditions

Before configuring the log sending interval when receiving the invalid packet, first complete the following task:

- Enable the interface security function.

Configure Log Sending Interval when Receiving Invalid Packet

The user can configure the log sending interval based on the actually received invalid packet. In the general application, just reserve the default value.

Table 55-11 Configure Log Sending Interval when Receiving Invalid Packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the log sending interval when receiving the invalid packet	**port-security violation log-interval** *log-interval-value*	Mandatory By default, the log sending interval when the interface receives the invalid packet securely is 5s.

55.2.7 Configure MAC+IP Rule for Accessing ACL Function ***-B -S -E -A***

Configuration Conditions

The following tasks have to be completed prior to the configuration of MAC+IP rules for using ACL functions:

- Enable port security function.

Configure MAC+IP rule for Accessing ACL Function

The user may, depending on actual needs, configure whether the MAC+IP rule uses ACL or not; if ALC is used, MAC+IP rule can precisely match the user's source MAC address with source IP address, prevent illegal users from accessing with matching source MAC address and mismatching source IP address.

Table 2-12 Configure the Handling Mode of Illegal Message

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2 ethernet interface configuration mode	**interface** *interface-name*	Must be chosen alternatively After entering L2 ethernet interface configuration mode, subsequent configurations only apply to current port; in aggregation group configuration mode, subsequent configurations only take effect in aggregation group
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure MAC+IP rule for accessing ACL function	**port-security use-acl**	Required By default, MAC+IP rules do not use ACL.

55.2.8 Monitoring and Maintaining of Port Security *-B -S -E -A*

Table 55-12 Monitoring and Maintaining of the Port Security

Command	**Description**
show port-security	Display the summary information of the port configured with the port security
show port-security ip-address	Display the configured IP rule
show port-security mac-address	Display the configured MAC rule and STICKY rule
show port-security active-address	Display the information of all effective entries

Command	Description
show port-security detect-mac	Display the currently detected new MAC entry
show port-security violation log-interval	Display the log print period when the invalid MAC entry is detected currently
show port-security violation-mac	Display the currently detected invalid MAC entry

55.3 Typical Configuration Example of Port Security

55.3.1 Configure MAC and IP Rule of Port Security *-B -S -E -A*

Network Requirements

- PC1, PC2 and the network printer are connected to the server via Device.
- Configure the port security function on Device, permitting PC1 to pass and refusing PC2 to pass; permit the network printer to execute the printing tasks delivered by the server and PC1 user.

Network Topology

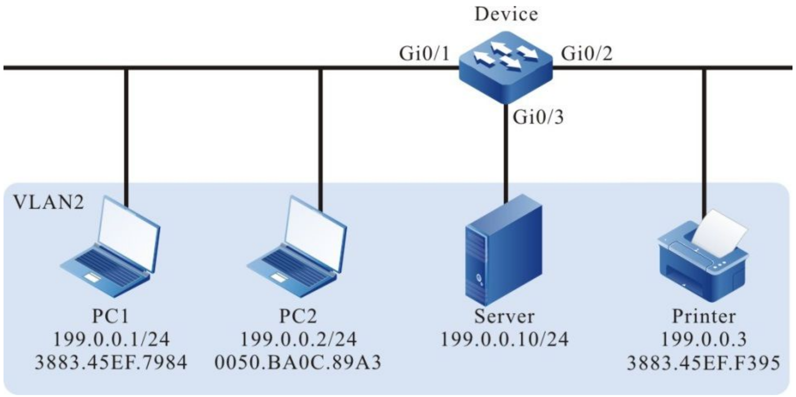


Figure 55–1 Networking of Configuring Port Security MAC and IP Rule

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port VLAN mode on gigabitethernet0/1-gigabitethernet0/3 of Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the port security function.

#Configure the MAC+IP rule on gigabitethernet0/1 of Device, permitting PC1 to pass; configure the IP rule, refusing PC2 to pass.

```
Device#config terminal
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security permit mac-address 3883.45ef.7984 ip-address 199.0.0.1
Device(config-if-gigabitethernet0/1)#port-security deny ip-address 199.0.0.2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the MAC rule on gigabitethernet0/2 of Device, permitting the network printer to access the network.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security enable
Device(config-if-gigabitethernet0/2)#port-security permit mac-address 3883.45ef.f395
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Check the result.

#View the effective entries of the port security on Device. The user can see that the MACs of PC1 and the network printer are written to the effective entries of the port security.

```
Device#show port-security active-address
-----------------------------------------------------------------------------------------
Entry Interface         MAC address      VID  IP Addr       Derivation     Age(Sec)
-----------------------------------------------------------------------------------------
1     gi0/1           38:83:45:EF:79:84 2    199.0.0.1      MAC+IP           0
2     gi0/2           38:83:45:EF:F3:95 2    199.0.0.3        MAC           0
```

#With the detection, we can see that PC1 can access the server and the network printer can execute the printing task delivered by PC1 and the server.

#With the detection, we can see that PC2 cannot ping the server or the network printer.

55.3.2 Configure MAX Rule of Port Security *-B -S -E -A*

Network Requirements

- PC1, PC2, and PC3 are connected to the server via Device; PC and the server are in the same LAN.
- Configure the port security rule on Device, permitting PC1 and PC2 to access the server and refusing PC3 to access the server.

Network Topology

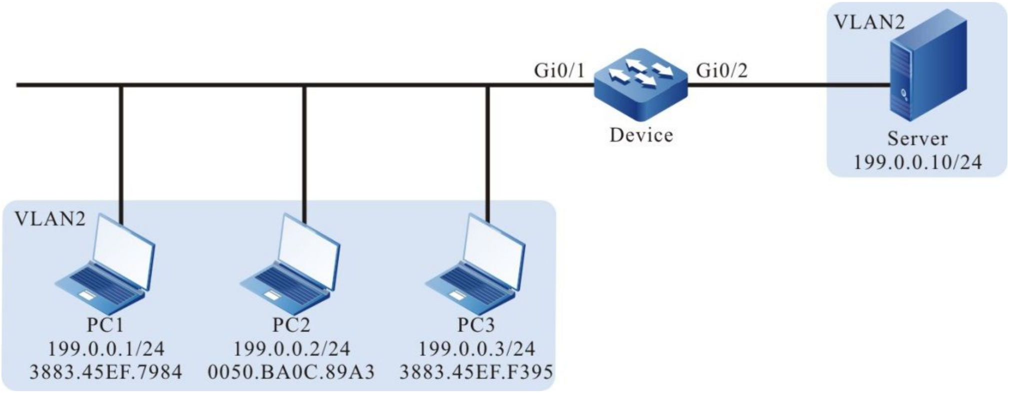


Figure 55–2 Networking of Configuring the MAX Rule of the Port Security

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port VLAN mode on gigabitethernet0/1-gigabitethernet0/2 of Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the port security rule on Device.

#Configure the MAX rule on gigabitethernet0/1 of Device. The maximum number of the MAC rules is 3.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security maximum 3
Device(config-if-gigabitethernet0/1)exit
```

#Refuse PC3 to access the server on giabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security deny mac-address 3883.45ef.f395
Device(config-if-gigabitethernet0/1)exit
```

Step 3: Check the result.

#The three PCs try to communicate with the server respectively. You can see that PC1 and PC2 can access the server and PC3 cannot access the server. View the effective entries of the port security on gigabitethernet0/1 of Device and you can see that the MAC addresses of PC1 and PC2 are written to the effective entries of the port security.

```
Device#show port-security active-address
------------------------------------------------------------------------------------------
```

```
Entry Interface          MAC address       VID  IP Addr       Derivation     Age(Sec)
---------------------------------------------------------------------------------------
1     gi0/1              00:50:ba:0c:89:a3 2    ---           FREE            0
2     gi0/1              38:83:45:EF:79:84 2    ---           FREE            0
Total Mac Addresses for this criterion: 2
```

55.3.3 Configure STICKY Rule of Port Security *-B -S -E -A*

Network Requirements

- PC1, PC2 and PC3 are connected to the server via Device; they are in the same LAN as the server.
- Configure the port security rule on Device, permitting two PCs to pass.
- After saving the configuration and restarting Device, the STICKY rule can take effect at once.

Network Topology

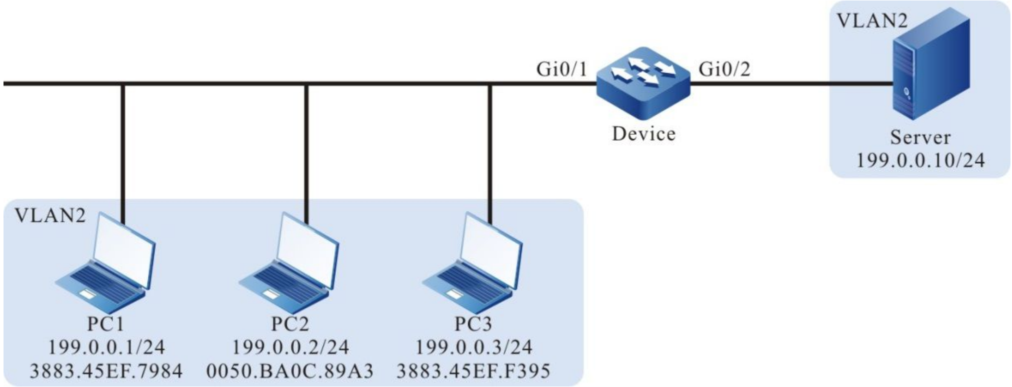


Figure 55–3 Networking of Configuring the STICKY Rule of the Port Security

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port VLAN mode on gigabitethernet0/1-gigabitethernet0/2 of Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the MAX rule of the port security on Device.

#Configure the MAX rule on gigabitethernet0/1 of Device. The maximum number of the MAX rules is 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security maximum 2
Device(config-if-gigabitethernet0/1)exit
```

Step 3: Configure the STICKY rule of the port security on Device.

#Enable the STICKY function on gigabitethernet0/1 of Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#port-security permit mac-address sticky
Device(config-if-gigabitethernet0/1)#exit
```

Step 4: Check the result.

#PC1, PC2 and PC3 try to communicate with the server. View the effective entries of the port security on gigabitethernet0/1 of Device and you can see that the rule type on gigabitethernet0/1 is STICKY.

```
Device#show port-security active-address
------------------------------------------------------------------------------------------
Entry Interface          MAC address       VID  IP Addr        Derivation       Age(Sec)
------------------------------------------------------------------------------------------
1    gi0/1             38:83:45:EF:79:84 2    199.0.0.1       STICKY           0
2    gi0/1             38:83:45:EF:F3:95 2    199.0.0.3       STICKY           0
Total Mac Addresses for this criterion: 2
```

#After saving the configuration and restarting the device, the STICKY rule exists and takes effect.

```
Device#show port-security active-address
------------------------------------------------------------------------------------------
Entry Interface          MAC address       VID  IP Addr        Derivation       Age(Sec)
------------------------------------------------------------------------------------------
1    gi0/1             38:83:45:EF:79:84 2    199.0.0.1       STICKY           0
2    gi0/1             38:83:45:EF:F3:95 2    199.0.0.3       STICKY           0
Total Mac Addresses for this criterion: 2
```

56 IP Source Guard

56.1 Overview

The IP Source Guard function is one packet filter function and can filter and control the packets forwarded by the port, preventing the invalid packets from passing the port and improving the port security. The function can be divided to two kinds:

1. The port IP Source Guard function filters the IP packets received by the specified port. The filter mode includes IP+VLAN and IP+MAC+VLAN. The specific processing modes are as follows:

- IP+VLAN mode: If the source IP address and VLAN ID in the packet are the same as the IP address and VLAN ID recorded in the bound entries, the port forwards the packet. Otherwise, drop it.
- IP+MAC+VLAN mode: If the source IP address, source MAC address, and VLAN ID in the packet are the same as the IP address, MAC address and VLAN ID recorded in the bound entries, the port forwards the packet. Otherwise, drop the packet.

The bound entries of the port IP Source Guard include two kinds:

- Static bound entries, manual configured port IP Source Guard static bound entries
- Dynamic bound entries, dynamically generated by the valid entries of the DHCP Snooping function.

2. Global IP Source Guard function filters the packets received by all ports, including ARP and IP packets. The specific filter modes are as follows:

- If the source IP address in the IP packet is the same as the IP address in the global IP Source Guard bound entries, but the source MAC address is different, drop the packet.
- If the sending IP address in the ARP packet is the same as the IP address in the bound entries, but the source MAC address is different, drop the packet.

56.2 IP Source Guard Function Configuration

Table 56-1 The Configuration List of the IP Source Guard Function

Configuration Task	
Configure the static bound entries of the port IP Source Guard	Configure the static bound entries of the port IP Source Guard
Configure the port IP Source Guard function	Configure the port IP Source Guard function

Configuration Task	
Configure the global IP Source Guard function	Configure the global IP Source Guard function

56.2.1 Configure Static Bound Entries of Port IP Source Guard *-B -S -E -A*

Configuration Conditions

Before configuring the static bound entries of the port IP Source Guard, first complete the following task:

- Enable the port IP Source Guard function or enable the port Dynamic ARP Inspection function

Configure Static Bound Entries of Port IP Source Guard

The static bound entries of the port IP Source Guard are the basis of filtering the IP packets received by the specified port.

When the port Dynamic ARP Inspection function is enabled, the static bound entries of the port IP Source Guard are the basis of the validity detection for the ARP packets.

Table 56-2 Configure Static Bound Entries of the Port IP Source Guard

Step	Command	Description
Enter global configuration mode	**config terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the static bound entries of the port IP Source Guard	**ip source binding** *mac-address* **vlan** *vlan-id ip-address*	Mandatory By default, there is no static bound entry of the port IP Source Guard.

NOTE

- For the port Dynamic ARP Inspection function, refer to the Dynamic ARP Inspection chapter of the configuration manual.

56.2.2 Configure Port IP Source Guard Function -B -S -E -A

Configuration Conditions

None

Configure Port IP Source Guard Function

After enabling the port IP Source Guard function, first write the port bound entry to the chip, including the static bound entry and dynamic bound entry. The static bound entry is first written. And then perform the security control for the IP packets received by the port according to the entries written to the chip, improving the security.

Table 56-3 Configure Port IP Source Guard Function

Step	Command	Description
Enter global configuration mode	**config terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the port IP Source Guard function	**ip verify source** [**ip-mac**]	Mandatory By default, the port IP Source Guard function is disabled. When the command does not carry the parameters, the filter mode for the IP packets is IP+VLAN; when the command

Step	Command	Description
		carries the parameters, the filter mode for the IP packet is IP+MAC+VLAN.

NOTE

- After enabling the port IP Source Guard function, the bound entries of the port IP Source Guard are written to the chip. The number of the entries written to the chip depends on the available chip entry resources. If the chip entry resources are used up and it is necessary to add bound entries or enable the port IP Source Guard function on the other port, we need to delete the related bound entries of some chip entry resources.
- If some port IP Source Guard bound entries cannot written to the chip because the chip entry resources are not enough, the system automatically try to write the bound entries to the chip again every 60s until all the bound entries are written to the chip or deleted.
- If the port IP Source Guard and global IP Source Guard functions are used at the same time, the IP packet received by the port needs to match the bound entries of the port IP Source Guard and global IP Source Guard so that it can be forwarded. Otherwise, it is dropped.
- Before enabling the port IP Source Guard function and if the terminal device connected to the port is non-DHCP client, or the terminal device is the DHCP client, but the local device does not enable the DHCP Snooping function, we need to configure the MAC address, IP address and the VLAN ID of the terminal device as the port IP Source Guard static bound entry, so as to ensure that after enabling the function, the terminal device communicates normally. For the DHCP Snooping function, refer to the DHCP Snooping chapter of the configuration manual.

56.2.3 Configure Port IP Source Guard Filter Message Type *-B -S -E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of port IP Source Guard filter message types:

- Enable port IP Source Guard function

Configure Port IP Source Guard Filter Message Type

After port IP Source Guard function has been enabled, filter IP messages in ip mode. Only when the port receives an IPv4 message in which the source IP address and VLAN ID are identical to the source IP address and VLAN ID in the port IP Source Guard binding table entries, the port will forward the message; otherwise, the message will be discarded.

After port IP Source Guard function has been enabled, filter IP messages in ip-mac mode. Only when the port receives an IP message in which the source MAC address, source IP address and VLAN ID are identical to the MAC address, IP address and VLAN ID in the port IP Source Guard binding table entries, the port will forward the message; otherwise, the message will be discarded.

After port IP Source Guard function has been enabled, filter IP messages in mac mode. Only when the port receives an IP message in which the source MAC address and VLAN ID are identical to the MAC address, IP address and VLAN ID in the port IP Source Guard binding table entries, the port will forward the message; otherwise, the message will be discarded.

Table 3-4 Configure Port IP Source Guard Filter Message Type

Steps	Command	Description
Enter global configuration mode	**config terminal**	-
Enter L2 ethernet interface configuration mode	**interface** *interface-name*	Must be chosen alternatively After entering L2 ethernet interface configuration mode, subsequent configurations only apply to current port; in aggregation group configuration mode, subsequent configurations only take effect in aggregation group
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable port IP Source Guard function	**ip verify source type {ip | ip-mac | mac}**	Required By default, filtration of ip filter type only works for dynamic table entries

56.2.4 Configure Port MAC Static Table Entry Binding Function *-B -S -E -A*

Configuration Conditions

The following tasks have to be completed prior to the configuration of port MAC static table entry binding function:

- Enable port IP Source Guard function

Configure Port MAC Static Table Entry Binding Function

After the port MAC static table entry binding function is configured, corresponding MAC address, vlan ID, and port ID will be obtained from the IP Source Guard static table entries configured on the port and the acquired dynamic table entries for delivering to corresponding static MAC table entries

Table 3-5 Configure MAC Static Table Entry Binding Function

Steps	Command	Description
Enter global configuration mode	**config terminal**	-
Enter L2 ethernet interface configuration mode	**interface** *interface-name*	Must be chosen alternatively After entering L2 ethernet interface configuration mode, subsequent configurations only apply to current port; in aggregation group configuration mode, subsequent configurations only take effect in aggregation group
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable port IP Source Guard function	**ip source sticky-mac**	Required By default, port MAC static table entry binding function is disabled

56.2.5 Configure Global IP Source Guard Function *-B -S -E -A*

Configuration Conditions

None

Configure Global IP Source Guard Function

To protect the security of the user IP address and prevent other user from using its own IP address, we can configure the global IP Source Guard function to bind the user IP address and MAC address. The global IP Source Guard bound entries of the configured user IP address and MAC address are directly written to the chip, so as to filter the invalid IP and ARP packets.

When enabling the global Dynamic ARP Inspection function, the configured global IP Source Guard bound entries serve as the basis of the validity detection of the global Dynamic ARP Inspection function for the ARP packets.

Table 56-4 Configure Global IP Source Guard Function

Step	**Command**	**Description**
Enter global configuration mode	**config terminal**	-

Step	Command	Description
Configure the global IP Source Guard function	**source binding** *mac-address ip-address*	Mandatory By default, there is no global IP Source Guard bound entry and the function is disabled. The command enables the global IP Source Guard function. Meanwhile, one global IP Source Guard bound entry is configured.

NOTE

- If Hybrid extended ACL is applied to the global (all ports) ingress, we need to cancel the application so that the global IP Source Guard function can be configured. Otherwise, the configuration fails. Refer to the ACL chapter of the configuration manual.
- The global IP Source Guard bound entries support 40 at most. After exceeding 40, the configuration fails.
- The configured global IP Source Guard bound entries are directly written to the chip. The number of the bound entries written to the chip depends on the available chip entry resources. If the chip entry resources are used up and it is necessary to add the global IP Source Guard bound entries, we need to delete the related bound entries of some chip entry resources.
- If the port IP Source Guard and global IP Source Guard functions are used at the same time, the IP packet received by the port needs to match the bound entries of the port IP Source Guard and global IP Source Guard so that it can be forwarded. Otherwise, it is dropped.

NOTE

- For the port Dynamic ARP Inspection function, refer to the Dynamic ARP Inspection chapter of the configuration manual.

56.2.6 IP Source Guard Monitoring and Maintaining *-B -S -E -A*

Table 56-5 IP Source Guard Monitoring and Maintaining

Command	Description
show ip binding table [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **slot** | **summary**]	Display the statistics information of the port IP Source Guard bound entries and the bound entry quantity
show ip source guard [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display the configuration information of the port IP Source Guard function
show source binding	Display the statics information of the global IP Source Guard bound entries and the entry quantity

56.3 Typical Configuration Example of IP Source Guard

56.3.1 Configure Port IP Source Guard Function Based on IP+VLAN

-B -S -E -A

Network Requirements

1. PC1 and PC2 are connected to IP Network via Device.
2. Configure the port IP Source Guard function based on IP+VLAN, realizing that PC1 can access IP Network normally and PC2 cannot access IP Network.

Network Topology

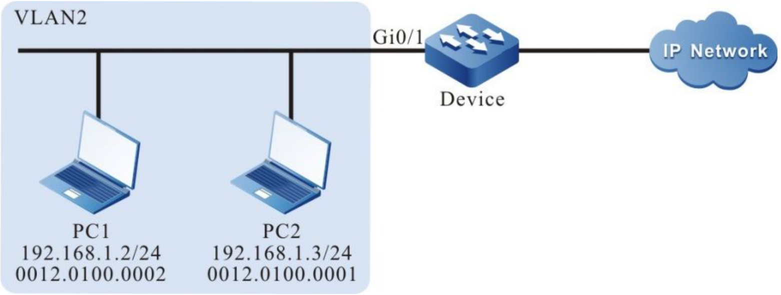


Figure 56–1 Networking of Configuring Port IP Source Guard Function Based on IP+VLAN

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the port IP Source Guard function on Device.

#Enable the port IP Source Guard function based on IP+VLAN on port gigabitethernet0/1, and configure the MAC address as 0012.0100.0001, IP address as 192.168.1.2, and the port IP Source Guard bound entry with VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip verify source
Device(config-if-gigabitethernet0/1)#ip source binding 0012.0100.0001 vlan 2 192.168.1.2
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View the configuration information of IP Source Guard.

```
Device#show ip source guard

-----------------------------------------
IP source guard interfaces on slot 0 :
   Total number of enabled interfaces : 1
-------------------------------------------------------
Interface Name       Status       Verify Type
-------------------------------------------------------
gi0/1              Enabled      IP
gi0/2              Disabled     Unknown
gi0/3              Disabled     Unknown
gi0/4              Disabled     Unknown
… …
```

We can see that the IP Source Guard function based on IP+VLAN is enabled on port gigabitethernet0/1.

#View the port IP Source Guard bound entry.

```
Device#show ip binding table
------------------------------------------
IP Source Guard binding table on slot 0
    Total binding entries     : 1
    Static binding entries    : 1
    Static not write entries  : 0
    Dynamic binding entries   : 0
    Dynamic not write entries : 0
    PCE writing entries       : 1
-----------------------------------------------------------------------------------------------
Interface-Name     MAC-Address     IP-Address     VLAN-ID Type-Flag     Writing-Flag    Entry-ID(H)
-----------------------------------------------------------------------------------------------
gi0/1            0012.0100.0001  192.168.1.2     2      Static        Wrote          65536
```

#PC1 can access IP Network normally and PC2 cannot access IP Network.

56.3.2 Configure Port IP Source Guard Function Based on MAC+VLAN

Network Requirements

- PC1, PC2 access IP Network via Device.
- Configure MAC+VLAN based port IP Source Guard function, so that PC1 can access IP Network normally but PC2 cannot access IP Network.

Network Topology

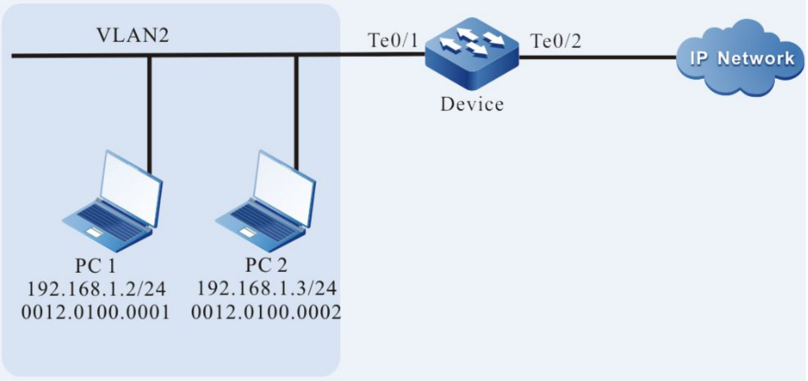


Figure 3-2 Networking Diagram - Configure MAC+VLAN Based Port IP Source Guard Function

Configuration Steps

Step 1: On the Device, configure VLAN and the port link types.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure port tengigabitethernet0/1's link type as Access to allow the pass of VLAN2 business.

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#switchport mode access
Device(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

Step 2: On the Device, configure port IP Source Guard function.

#On port tengigabitethernet0/1, enable MAC+VLAN based filter mode port IP Source Guard function, and configure MAC address to 0012.0100.0001, VLAN2's port IP Source Guard binding table entry.

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip verify source
Device(config-if-tengigabitethernet0/1)#ip source binding mac-address 0012.0100.0001 vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

Step 3: Check the result.

#Check IP Source Guard related configuration information.

```
Device#show ip source guard
----------------------------------------
IP source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
------------------------------------------------------------
```

```
Interface Name          Status       Verify Type  L2 Status
-------------------------------------------------------------
te0/1                   Enabled      IP         Disabled
te0/2                   Disabled     IP         Disabled
te0/3                   Disabled     IP         Disabled
te0/4                   Disabled     IP         Disabled
……
```

It can be seen that IP Source Guard function has already been enabled on port tengigabitethernet0/1; static IP Source Guard table entries will take effect depending on the configured MAC+VLAN table entries and have nothing to do with the Verify Type value. The above example is valid based on MAC+VLAN.

#Check port IP Source Guard binding table entries.

```
Device#show ip binding table
-------------------------------------------
IP Source Guard binding table on slot 0
    Total binding entries      : 1
    Static binding entries     : 1
    Static not write entries  : 0
    Dynamic binding entries    : 0
    Dynamic not write entries : 0
    PCE writing entries        : 1
------------------------------------------------------------------------------------------
Interface-Name  MAC-Address    IP-Address   VLAN-ID   Type-Flag   Writing-Flag   L2-Flag
------------------------------------------------------------------------------------------
te0/1         0012.0100.0001     ---        2        Static      Wrote       Not Write
```

#PC1 can access IP Network normally, PC2 cannot access IP Network.

56.3.3 Configure Port IP Source Guard Function Based on IP+MAC+VLAN

-B -S -E -A

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure the port IP Source Guard function based on IP+MAC+VLAN, realizing that PC1 can access IP Network normally and PC2 cannot access IP Network.

Network Topology

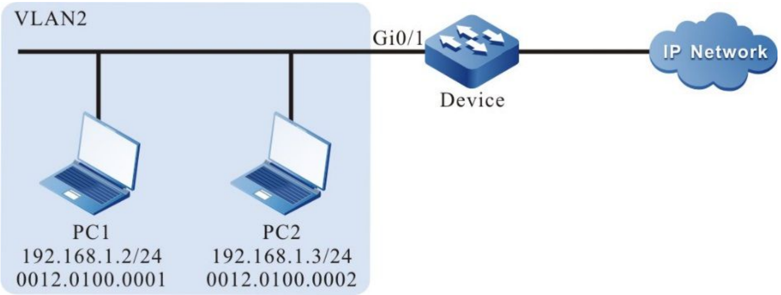


Figure 56–2 Networking of Configuring Port IP Source Guard Function Based on IP+MAC+VLAN

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the port IP Source Guard function on Device.

#Enable the port IP Source Guard function based on IP+MAC+VLAN on port gigabitethernet0/1, and configure the MAC address as 0012.0100.0001, IP address as 192.168.1.2, and the port IP Source Guard bound entry with VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip verify source ip-mac
Device(config-if-gigabitethernet0/1)#ip source binding 0012.0100.0001 vlan 2 192.168.1.2
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View the configuration information of IP Source Guard.

```
Device#show ip source guard

-----------------------------------------
IP source guard interfaces on slot 0 :
   Total number of enabled interfaces : 1
-------------------------------------------------------
Interface Name       Status       Verify Type
-------------------------------------------------------
gi0/1              Enabled      IP+MAC
gi0/2              Disabled     Unknown
gi0/3              Disabled     Unknown
gi0/4              Disabled     Unknown
… …
```

We can see that the IP Source Guard function based on IP+MAC+VLAN is enabled on port gigabitethernet0/1.

#View the port IP Source Guard bound entry.

```
Device#show ip binding table
------------------------------------------
IP Source Guard binding table on slot 0
    Total binding entries     : 1
    Static binding entries    : 1
    Static not write entries  : 0
    Dynamic binding entries   : 0
    Dynamic not write entries : 0
    PCE writing entries       : 1
-----------------------------------------------------------------------------------------------
Interface-Name      MAC-Address     IP-Address      VLAN-ID Type-Flag      Writing-Flag    Entry-ID(H)
-----------------------------------------------------------------------------------------------
```

```
               gi0/1           0012.0100.0001  192.168.1.2     2       Static          Wrote           65536
```

#PC1 can access IP Network normally and PC2 cannot access IP Network.

57 DHCP snooping

57.1 Overview

57.1.1 Overview of DHCP snooping Basic Functions *-B -S -E -A*

DHCP snooping is one security feature of DHCP (Dynamic Host Configuration Protocol) and has the following two functions:

1. Record the corresponding relation of the MAC address and IP address of the DHCP client:

Considering the security, the network administrator may need to record the IP address used when the user accesses the network, confirming the corresponding relation of the user host IP address and the IP address got from the DHCP server.

DHCP snooping listens to the DHCP request packet and the DHCP response packet received by the trust port and records the MAC address of the DHCP client and the obtained IP address. The administrator can view the IP address information got by the DHCP client via the bound entry recorded by DHCP snooping.

2. Ensure that the client gets the IP address from the valid server

If there is unauthorized DHCP server in the network, the DHCP client may get the wrong IP address, resulting in the communication abnormality or security risks. To ensure that the DHCP client can get the IP address from the valid DHCP server, the DHCP snooping function permits configuring the port as the trust port or un-trust port:

- Trust port is the port directly or indirectly connected to the valid DHCP server. The trust port forwards the received DHCP response packet normally, so as to ensure that the DHCP client can get the correct IP address.
- Un-trust port is the port not directly or indirectly connected to the valid DHCP server. If the un-trust port receives the DHCP response packet sent by the DHCP server, drop it, so as to prevent the DHCP client from getting the wrong IP address.

57.1.2 Brief Introduction of DHCP snooping Option82 *-B -S -E -A*

DHCP snooping supports the adding, forwarding and managing for the Option82. Option82 is one DHCP packet option. The option is used to record the location information of the DHCP client and the administrator can locate the DHCP client according to the option, so as to perform some security control. For example, control the number of the IP addresses that can be distributed to one port or VLAN. The processing mode of Option82 varies with the DHCP packet type:

1. After the device receives the DHCP request packet, process the packet according to whether the packet contains the Option82, the processing policy configured by the user and the filling format, and then forward the processed packet to the DHCP server.

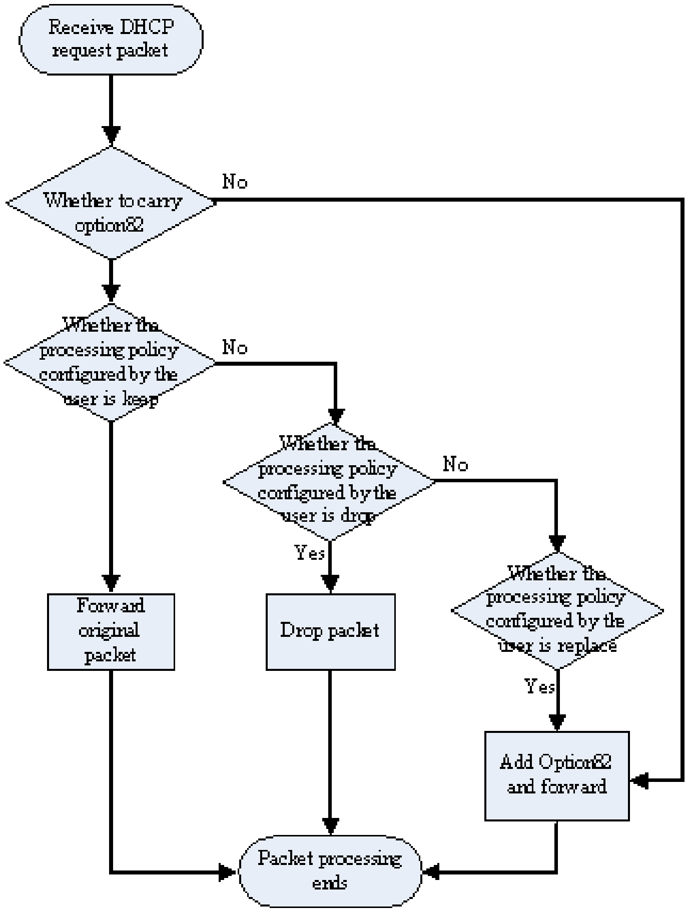

Receive DHCP request packet
Whether to carry option82
No
Whether the processing policy configured by the user is keep
No
Whether the processing policy configured by the user is drop
No
Yes
Whether the processing policy configured by the user is replace
Yes
Forward original packet
Drop packet
Add Option82 and forward
Packet processing ends

Figure 57-1 Processing Flow of Option82

2. When the device receives the response packet of the DHCP server and if the packet contains the Option82, delete the Option82 and forward to the DHCP client; if the packet does not contain the Option82, directly forward to the DHCP client.

57.2 DHCP snooping Function Configuration

Table 57-1 DHCP snooping Function Configuration List

Configuration Task	
Configure the DHCP snooping basic functions	Configure the DHCP snooping function
	Configure the port trust status
	Configure the DHCP snooping rate limitation function
Configure DHCP snooping Option82	Configure the Remote ID content
	Configure the Circuit ID content

Configuration Task	
	Configure the filling format of the Option82
	Configure the processing policy of the Option82 packet
Configure the storing of the DHCP snooping bound entries	Configure the auto storing of the DHCP snooping bound entry
	Configure the manual storing of the DHCP snooping bound entry

57.2.1 Configure DHCP snooping Basic Functions *-B -S -E -A*

The DHCP snooping basic functions include enabling the DHCP snooping function, configuring the port trust status and limiting the rate of the DHCP packets.

Configuration Conditions

None

Configure DHCP snooping Function

After enabling the DHCP snooping function, monitor the DHCP packets received by all the ports of the device:

1. For the received request packet, generate the corresponding bound entry according to the information in the packet
2. For the response packet received from the trust packet, update the status and lease time of the bound entry
3. For the response packet received from the un-trust port, directly drop it

Table 57-2 Configure DHCP snooping Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable the DHCP snooping function	**dhcp-snooping**	Mandatory By default, DHCP snooping function is disabled.

Configure Port Trust Status

To prevent the DHCP client from getting the address from the invalid DHCP server, we can configure the port directly or in-directly connected to the valid server as the trust port.

After the port is configured as the trust port, permit the normal forwarding of the DHCP response packet. Otherwise, drop the DHCP response packet.

Table 57-3 Configure Port Trust Status

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the port trust status	**dhcp-snooping trust**	Mandatory By default, all ports are un-trust port.

NOTE

- The port connected to the DHCP server needs to be configured as the trust port. Otherwise, the DHCP client cannot get the address.
- After the port is configured as the trust port, do not limit the rate of the DHCP packets passing the port.
- After changing the port status from the trust port to the un-trust port, the upper threshold of the port rate is the default 40.

Configure DHCP snooping Rate Limitation

Configuring the DHCP snooping rate limitation function can limit the number of the DHCP packets processed every second, avoiding that other protocol packets cannot be processed in time because the system processes the DHCP packets for a long time.

When the number of the DHCP packets received within one second exceeds the rate limitation, the subsequent DHCP packets are dropped. If the DHCP packets received by the port for successive 20s exceed the rate limitation, disable the port to isolate the packet impact source.

Table 57-4 Configure DHCP snooping Rate Limitation Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the DHCP snooping rate limitation function	**dhcp-snooping rate-limit** *limit-value*	Mandatory By default, the upper rate threshold of the DHCP packets is 40pps.

NOTE

- After configuring the rate threshold of the DHCP packets in the aggregation group configuration mode, the DHCP packet rate threshold of each member port of the aggregation group is the value.
- The DHCP packet rate limitation function just takes effect for the un-trust port and does not take effect for the trust port.
- After the port is disabled automatically, we can configure Error-Disable to enable the port automatically. By default, the auto disabling function of the port is enabled; if the DHCP packets received by the port for successive 20s exceed the rate limitation, but cannot disable the port automatically, we need to view the configuration of Error-Disable. For the Error-Disable function, refer to the Error-Disable chapter of the configuration manual.

57.2.2 Configure DHCP snooping Option82 *-B -S -E -A*

The DHCP snooping function supports Option82. Option82 can contain 255 sub options at most. MTS device supports two sub options, that is, Circuit ID and Remote ID.

Configuration Conditions

Before configuring DHCP snooping Option82, first complete the following task:

- Enable the DHCP snooping function

Configure Remote ID

The content of Remote ID includes default content and non-default content. The filling format of the default content of Remote ID is as follows:

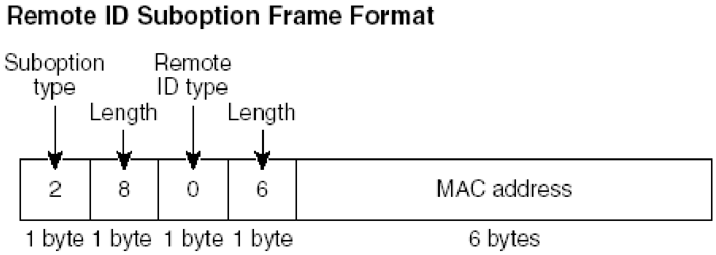


Figure 57-2 The Filling Format of the Default Content of Remote ID

The non-default content includes customized character string and device name, and needs to be configured to take effect in the user configuration format. The filling format of the non-default content of Remote ID is as follows:

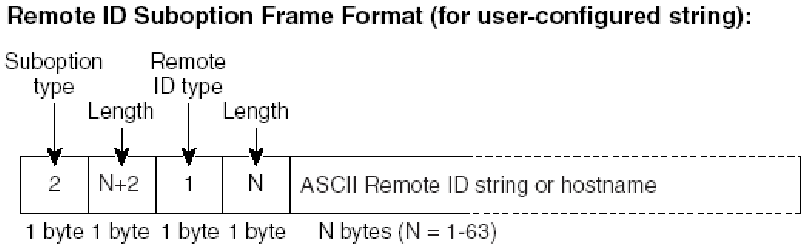

Remote ID Suboption Frame Format (for user-configured string):
Suboption type
Length
Remote ID type
Length
2
N+2
1
N
ASCII Remote ID string or hostname
1 byte
1 byte
1 byte
1 byte
N bytes (N = 1-63)

Figure 57-3 The Filling Format of the Non-Default Content of Remote ID

Table 57-5 Configure the Content of Remote ID

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the content of Remote ID	**dhcp-snooping information format remote-id** { *string* | **default** | **hostname** }	Mandatory By default, the content of Remote ID is the default content, that is, the MAC address of the device port.

Configure Circuit ID

The content of Circuit ID includes default content and non-default content. The filling format of the default content of Circuit ID is as follows:

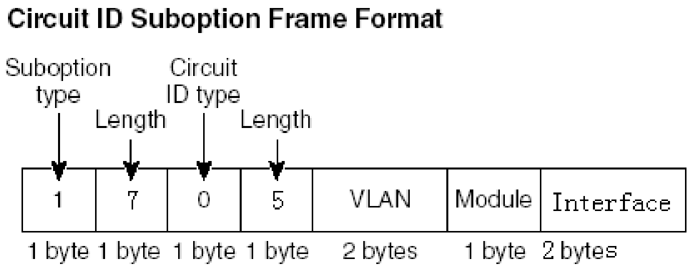


Figure 57-4 The filling format of the default content of Circuit ID

The non-default content needs to be configured to take effect in the user configuration format. The filling format of the non-default content of Circuit ID is as follows:

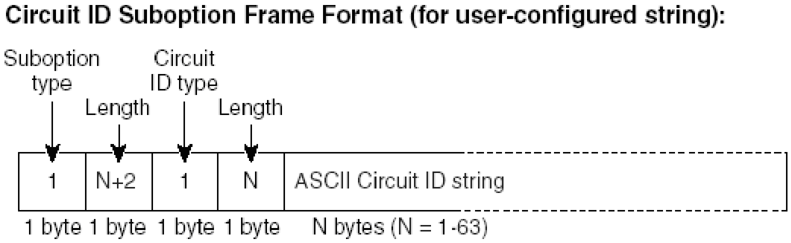


Figure 57-5 The Filling Format of the Non-Default Content of Circuit ID

Table 57-6 Configure the Content of Circuit ID

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the content of Circuit ID	**dhcp-snooping information format circuit-id** { *string* | **default** }	Mandatory By default, the content of Circuit ID is the default content.

Configure Filling Format of Option82

The filling format of Option82 includes default format and user configuration format.

When the filling format is the default format, the contents of Remote ID and Circuit ID are both default content; only after the filling format is configured as the user configuration format, the non-default contents of Remote ID and Circuit ID can take effect.

Table 57-7 Configure Filling Format of Option82

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the filling format of Option82	**dhcp-snooping information format** { **default** | **user-config** }	Mandatory By default, the filling format is the default format.

Configure Packet Processing Policy of Option82

Configure the packet processing policy of Option82. We can adopt different forwarding policies for the DHCP request packet containing Option82.

Table 57-8 Configure Packet Processing Policy of Option82

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the packet processing policy of Option82	**dhcp-snooping information policy** { **drop** | **keep** | **replace** }	Mandatory By default, the processing policy is replace.

57.2.3 Configure Storing of DHCP snooping Bound Entries *-B -S -E -A*

The DHCP snooping function supports the auto or manual storing to the specified path of the bound entries. If the device restarts, the stored bound entries can be restored, avoiding affecting the communication because the bound entries are lost.

The specified path can be device FLASH, FTP server or TFTP server.

Configuration Conditions

Before configuring the storing path of the bound entries as the FTP/TFTP server, first complete the following task:

1. FTP/TFTP server, enable the FTP/TFTP server function normally
2. The device can ping the IP address of the FTP/TFTP server.

Configure Auto Storing of DHCP snooping Bound Entries

DHCP snooping bound entries can be configured as the auto storing mode, that is, system automatically stores the bound entries regularly.

The system periodically refreshes the bound entries, detecting whether the bound entries are updated. If yes, we need to store the updated entries to the specified path after the storing delay arrives. The storing delay can prevent and control the frequent storing of the system because the entries are updated continuously.

Table 57-9 Configure Auto Storing of DHCP snooping Bound Entries

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the auto storing of the DHCP snooping bound entries	**dhcp-snooping database savetype auto** { **flash** *file-name* | **ftp** *dest-ip-address ftp-username ftp-password file-name* | **tftp** *dest-ip-address file-name* }	Mandatory By default, the storing mode of the bound entries is auto mode, the storing path is flash, and the storing file name is dhcpsp_binding.db.
Configure the storing delay of the bound entries	**dhcp-snooping database savedelay** *seconds*	Optional By default, the storing delay of the bound entries is 1800s.
Configure the refresh interval of the bound entries	**dhcp-snooping database savepool** *seconds*	Optional By default, the refresh interval of the bound entries is 30s.

Configure Manual Storing of DHCP snooping Bound Entries

DHCP snooping bound entries can be configured as the manual storing mode, that is, execute the store command to complete the storing of the bound entries.

Table 57-10 Configure Manual Storing of DHCP snooping Bound Entries

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the manual storing of the DHCP snooping bound entries	**dhcp-snooping database savetype manual** { **flash** *file-name* | **ftp** *dest-ip-address ftp-username ftp-password file-name* | **tftp** *dest-ip-address file-name* }	Mandatory By default, the storing mode of the bound entries is auto mode, the storing path is flash and the storing file name is dhcpsp_binding.db.
Configure the storing bound file	**dhcp-snooping database save**	Mandatory Store the bound entries to the specified path. By default, the bound entries are not stored to the specified path.

57.2.4 Monitoring and Maintaining of DHCP snooping *-B -S -E -A*

Table 57-11 Monitoring and Maintaining of DHCP snooping

Command	Description
clear dhcp-snooping database { **interface** *interface-list* | **link-aggregation** *link-aggregation-id* | *mac-address* | **all** }	Clear the bound entries
show dhcp-snooping [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **save**]	Display the configuration information of DHCP snooping
show dhcp-snooping database [| { { **begin** | **exclude** | **include** } *expression* | **redirect** { **file** *file-name* | **ftp** [**vrf** *vrf-name*] { *hostname* | *dest-ip-address* } *ftp-username ftp-password file-name* } }] [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* [| { { **begin** | **exclude** | **include** } *expression* | **redirect** { **file** *file-name* |	Display the DHCP snooping bound entry information

Command	Description
ftp [**vrf** *vrf-name*] { *hostname* | *dest-ip-address* } *ftp-username ftp-password file-name* } }]]	

57.3 Typical Configuration Example of DHCP snooping

57.3.1 Configure DHCP snooping Basic Functions *-B -S -E -A*

Network Requirements

- DHCP Server1 is the valid DHCP server; DHCP Server2 is the invalid DHCP server.
- After configuring the DHCP snooping function, PC1 and PC2 both can get address from DHCP Server1.

Network Topology

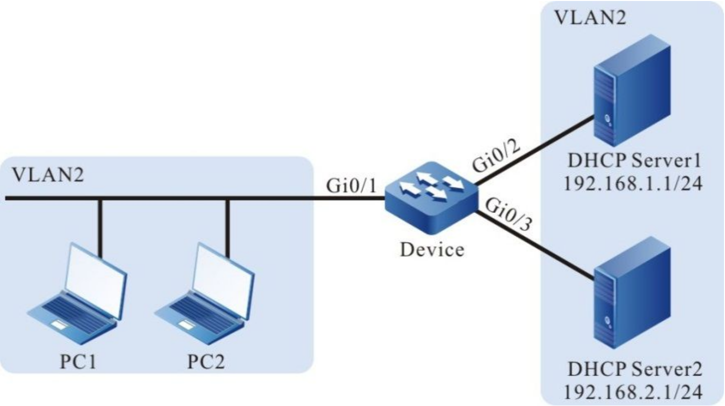


Figure 57-6 Networking of Configuring DHCP snooping Basic Functions

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1-gigabitethernet0/3 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the address pool of DHCP Server1 as 192.168.1.100-192.168.1.199 and the address pool of DHCP Server2 as 192.168.2.100-192.168.2.199. (Omitted)

Step 3: Configure the DHCP snooping function on Device.

#Enable the DHCP snooping function.

```
Device(config)#dhcp-snooping
```

#Configure the port gigabitethernet0/2 as trust port.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dhcp-snooping trust
Device(config-if-gigabitethernet0/2)#exit
```

Step 4: Check the result.

#After PC1 and PC2 get the address successfully, view the DHCP snooping entries on Device.

```
Device#show dhcp-snooping database
    dhcp-snooping database:
    database entries count:2
    database entries delete time :300
    ---------------------------------
    macAddr         ipAddr          transtion-id    vlan   interface        leaseTime(s)    status
    0013.0100.0002  192.168.1.101   1               2      gi0/1            107990          active
    ------
    0013.0100.0001  192.168.1.100   0               2      gi0/1            107989          active
    ------
Total valid DHCP Client binding table for this criterion: 2
```

PC1 and PC2 both can get address from DHCP Server1.

58 Dynamic ARP Inspection

58.1 Overview

Dynamic ARP Inspection is called DAI for short. Discover and prevent the ARP spoofing attack by checking the validity of the ARP packet, improving the network security. The DAI function is divided to two kinds:

1. Port DAI function: Check the validity of the ARP packet received by the specified port, so as to discover and prevent the ARP spoofing attack;

The basis of checking the validity of the ARP packet is the port IP Source Guard bound entry. The specific checking principle is as follows:

If the sending IP address, source MAC address and VLAN ID in the received ARP packet match with the port IP Source Guard bound entries, the ARP packet is valid packet and forward it. Otherwise, the ARP packet is invalid packet, drop it, and record the log information.

2. Global DAI function: Check the validity of the ARP packets received by all ports, preventing the counterfeiting users from sending the fake ARP packets and the device sets up the wrong ARP entry.

The basis of the ARP packet validity inspection is the global IP Source Guard bound entries. The specific detecting principle is as follows:

When the sending IP address in the received ARP packet is the same as the IP address in the global IP Source Guard bound entries, but the source MAC address is different, the ARP packet is fake packet, drop it and do not record the log information.

The port DAI and global DAI functions also check the effectiveness of the ARP packet. The specific checking principle is as follows:

When the source MAC address in the received ARP packet is different from the sending MAC address, the packet is ineffective packet, drop it and do not record the log information.

- Interface ARP Attack Detection: Do not perform validation detection for the ARP packet received on the specified interface. Only record the log information, which is used to detect the ARP attack.

58.2 Dynamic ARP Inspection Function Configuration

Table 58-1 The Configuration List of Dynamic ARP Inspection Function

Configuration Task	
Configure the port Dynamic ARP Inspection function	Configure the port Dynamic ARP Inspection function
Configure the global Dynamic ARP Inspection function	Configure the global Dynamic ARP Inspection function

58.2.1 Configure Port Dynamic ARP Inspection Function *-B -S -E -A*

Configuration Conditions

Before configuring the port Dynamic ARP Inspection function, first complete the following task:

- Configure the port IP Source Guard bound entries

Configure Port Dynamic ARP Inspection

After enabling the port DAI function, the system checks the validity of the ARP packet received by the port according to the port IP Source Guard bound entries. The invalid packet is dropped and recorded in the logs.

The contents recorded in the logs include VLAN ID, receiving port, sending IP address, destination IP address, sending MAC address, destination MAC address and the number of the same invalid ARP packets. The user can analyze further according to the recorded log information, such as locate the host initiating the ARP packet.

By default, the log information is output periodically. We can control the recording, outputting and aging of the packet by configuring the output interval of the log. The log output interval serves as the basis of the following log parameters:

- Log refresh period: Used to judge whether the logs need to output and age. If the configured log output interval is smaller than 5s, the log refresh period is equal to 1s. Otherwise, the log refresh period is equal to 1/5 of the log output interval.
- Log age time: After the age time times out, the logs are deleted. The log age time is two multiples of the log output interval.
- Log token: In the log refresh period, the maximum number of the logs permitted to be recorded. The number of the log tokens is 15 multiples of the log refresh period.

After enabling the port DAI function, we can also configure the port ARP rate limitation function, that is, limit the number of the ARP packets that are processed every second, avoiding that the other protocol packets cannot be processed in time because the system processes lots of ARP packets for a long time.

NOTE

- The port ARP rate limitation function is to limit the number of the ARP packets that are processed every second, avoiding that the other protocol packets cannot be processed in time because the system processes lots of ARP packets for a long time. After the number of the ARP packets received in one second exceeds the rate threshold, the subsequent received ARP packets are dropped. If the ARP packets received by the port in successive

15s exceed the rate, disable the port to isolate the packet impact source.

Table 58-2 Configure the Port Dynamic ARP Inspection Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the port DAI function	**ip arp inspection**	Mandatory By default, the port DAI function is disabled.
Configure the upper threshold of the ARP packets processed by the port	**ip arp inspection rate-limit** *limit-value*	Optional By default, the upper threshold of the ARP packets processed by the port is 15pps.
Return to the global configuration mode	**exit**	-
Configure the number of the buffered logs	**ip arp inspection log-buffer** *buffer-size*	Optional By default, the system can buffer 32 logs. If it is configured as 0, it indicates that the logs are not buffered, that is, after detecting the invalid ARP packet, the logs are directly output to the terminal.

Step	Command	Description
Configure the log output interval	**ip arp inspection log-interval** *seconds*	Optional By default, the log output interval is 20s. If it is configured as 0, it indicates that the logs are not buffered, that is, after detecting the invalid ARP packet, the logs are directly output to the terminal.
Configure the log output level	**ip arp inspection log-level** *log-level*	Optional By default, the log output level is 6.

NOTE

- After the port DAI function is enabled, all ARP packets received by the port (broadcast ARP and unicast ARP) are re-directed to the CPU for detecting, software forwarding, log recording and so on. When the number of the ARP packets is large, they seriously consume CPU resources, so when the device communicates normally, it is not suggested to enable the port DAI function. When it is doubted that there is ARP spoofing attack in the network, it is necessary to enable the port DAI function to detect and locate.
- In one port, the port DAI function cannot be used with the port security function at the same time.
- After configuring the rate threshold of the port processing the ARP packets in the aggregation group configuration mode, the ARP packet rate threshold of each member port of the aggregation group is the value.
- If the ARP packets received by the port in successive 20s exceed the upper threshold, but the port is not automatically disabled, it is necessary to refer to the Error-Disable chapter of the configuration manual.

58.2.2 Configure Global Dynamic ARP Inspection Function *-B -S -E -A*

Configuration Conditions

Before configuring the global Dynamic ARP Inspection function, first complete the following task:

- Configure the global IP Source Guard bound entry

Configure Global Dynamic ARP Inspection Function

After enabling the global DAI function, the system checks the validity of the received ARP packet according to the global IP Source Guard bound entries. The invalid packet is dropped and not recorded in the logs.

Table 58-3 Configure the Global Dynamic ARP Inspection Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable the global DAI function	**arp-security**	Mandatory By default, the global DAI function is disabled.

58.2.3 Configure Dynamic ARP Attack Inspection *-B -S -E -A*

Configuration Conditions

None

Configure Dynamic ARP Attack Inspection

After the dynamic ARP attack detection is enabled, the system will not perform the validation inspection for the received ARP packet but only record the log.

Table 58-4 Configure the dynamic ARP attack inspection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration can only take effect on the current interface. After entering the aggregation group configuration mode, the subsequent configuration can only take effect in the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Enable the ARP attack detection on the interface	**ip arp inspection attack**	Mandatory By default, the ARP attack detection is not enabled on the interface.

58.2.4 Monitoring and Maintaining of Dynamic ARP Inspection *-B -S -E -A*

Table 58-5 Dynamic ARP Inspection Monitoring and Maintaining

Command	Description
clear ip arp inspection { **log-information** | **log-statistics** }	Delete the log information recorded by the port DAI function
show arp-security	Display the status of the global DAI function
show ip arp inspection [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display the configuration information of the port DAI function
show ip arp inspection log-information	Display the log information recorded by the port DAI function
show ip arp inspection log-statistics	Display the statistics information of the logs

58.3 DAI Typical Configuration Example

58.3.1 Configure DAI Basic Functions *-B -S -E -A*

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure the port DAI function on Device, preventing the ARP attack and spoofing.

Network Topology

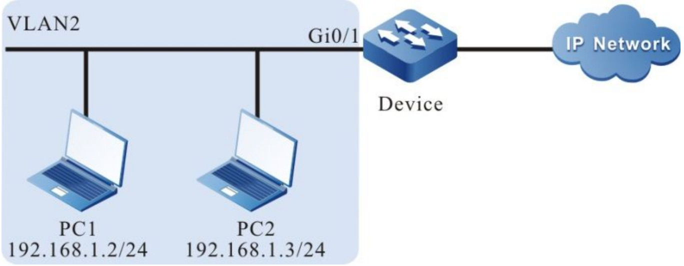


Figure 58–1 Networking of Configuring the DAI Basic Functions

Configuration Steps

Step 1: Configure the link type of the VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the port DAI function on Device.

#Enable the port DAI function on port gigabitethernet0/1 and configure the upper threshold of port gigabitethernet0/1 processing ARP packets as 30pps.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip arp inspection
Device(config-if-gigabitethernet0/1)#ip arp inspection rate-limit 30
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Configure the bound entries on Device.

#Configure the MAC address on port gigabitethernet0/1 as 0012.0100.0001, IP address as 192.168.1.2, and the port IP Source Guard bound entries with VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip source binding 0012.0100.0001 vlan 2 192.168.1.2
Device(config-if-gigabitethernet0/1)#exit
```

Step 4: Check the result.

#Configure the DAI configuration information.

```
Device#show ip arp inspection
    Dynamic ARP Inspection information:
    Dynamic ARP Inspection log buffer size: 30
    Dynamic ARP Inspection log Interval:    20
Dynamic ARP Inspection log Level:       6
Dynamic ARP Inspection interface information :
-------------------------------------------
interface           status    rate-limit(pps)  attack
gi0/1              enable    30              OFF
gi0/2              disable   15              OFF
……
```

#When the rate of the port gigabitethernet0/1 receiving the ARP packets exceeds 30pps, Device drops the excessive packets and outputs the following prompt information.

```
Jan  1 02:21:06: The rate on interface gigabitethernet0/1 too fast ,the arp packet drop!
```

#When the rate of the port gigabitethernet0/1 receiving the ARP packets exceeds 30pps for successive 20s, Device disables port gigabitethernet0/1 and outputs the following prompt information.

```
Jan  1 02:21:26: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Jan  1 02:21:26: The rate of arp packet is too fast,dynamic arp inspection shut down the gigabitethernet0/1 !
```

#When the ARP packets received by port gigabitethernet0/1 are inconsistent with the bound entries, Device records the following format of invalid information to the DAI logs and outputs regularly.

```
Jan  1 07:19:49:  SEC-7-DARPLOG: sender IP address: 192.168.1.3 sender MAC address:0011.0100.0001
target IP address: 0.0.0.0 target MAC address:0000.0000.0000 vlan ID:2 interface ID:gigabitethernet0/1 record
packet :32 packet(s)
```

#View the DAI logs.

```
Device#show ip arp inspection log-information
LogCountInBuffer:1

 SEC-7-DARPLOG: sender IP address: 192.168.1.3 sender MAC address:0011.0100.0001 target IP address:
0.0.0.0  target  MAC  address:0000.0000.0000  vlan  ID:2  interface  ID:gigabitethernet0/1  record  packet  :0
packet(s)
```

58.3.2 DAI Combining With DHCP Snooping   *-B -S -E -A*

Network Requirements

- PC1 and PC2 are connected to IP Network via Device; PC2 is the DHCP client; Device2 is the DHCP relay.
- Device1 configures DHCP Snooping and port DAI function, realizing that PC2 can access IP Network normally and PC1 cannot access IP Network.

Network Topology

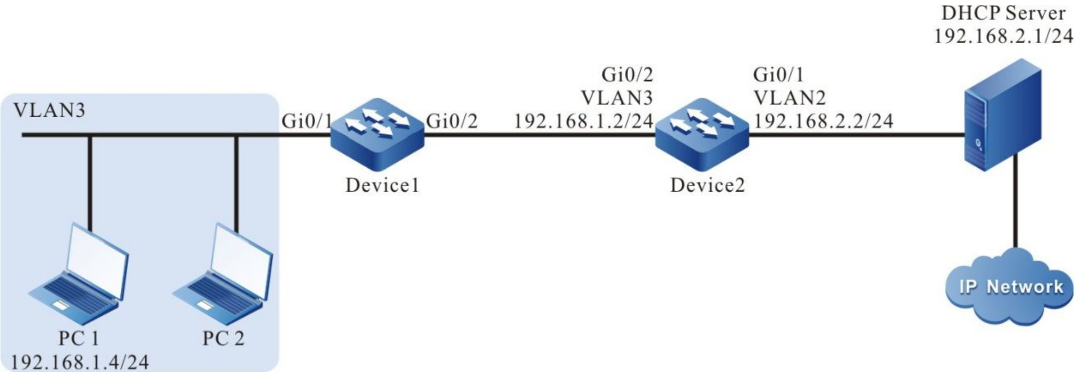


Figure 58–2 Networking of Combing DAI with DHCP Snooping

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device1.

#Create VLAN3.

```
Device1#configure terminal
Device1(config)#vlan 3
Device1(config-vlan3)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 as Access, permitting the services of VLAN3 to pass.

```
Device1(config)#interface gigabitethernet 0/1-0/2
Device1(config-if-range)#switchport access vlan 3
Device1(config-if-range)#exit
```

Step 2: Configure the link type of VLAN and port on Device2.

#Create VLAN2 and VLAN3.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 as Access; port gigabitethernet0/1 permits the services of VLAN2 to pass; port gigabitethernet0/2 permits the services of VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode access
Device2(config-if-gigabitethernet0/2)#switchport access vlan 3
Device2(config-if-gigabitethernet0/2)#exit
```

Step 3: Configure VLAN interface and IP address on Device1 and Device2. (Omitted)

Step 4: Configure the DHCP Snooping function on Device1.

#Enable the DHCP Snooping function and configure the port gigabitethernet0/2 as trust port.

```
Device1(config)#dhcp-snooping
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#dhcp-snooping trust
Device1(config-if-gigabitethernet0/2)#exit
```

Step 5: Configure the port DAI function on Device1.

#Enable the port DAI function on port gigabitethernet0/1.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#ip arp inspection
Device1(config-if-gigabitethernet0/1)#exit
```

Step 6: Configure the IP address of the DHCP relay server on Device2.

#Configure the IP address of the DHCP relay server as 198.168.2.1.

```
Device2(config)#ip dhcp-server 192.168.2.1
```

Step 7: Check the result.

#After PC2 gets the address successfully; view the DHCP Snooping dynamic entries on Device1.

```
Device1#show dhcp-snooping database
    dhcp-snooping database:
    database entries count:1
    database entries delete time :300
    ---------------------------------
    macAddr         ipAddr          transtion-id    vlan   interface        leaseTime(s)    status
    0013.0100.0001  192.168.1.100   2               2      gi0/1            107990          active
    ------
```

#PC2 can access IP Network normally and PC1 cannot access IP Network.

59 Host Guard

59.1 Overview

The Host Guard function is mainly used to the access layer devices, preventing the ARP packets forged by the attacker from damaging the ARP table on the terminal device. The host IP address protected by Host Guard is usually applied to the IP addresses of the gateway device in the network and important server.

In the Host Guard function, there are two concepts:

- Host Guard group: comprises a series of host guard group rules, that is, the set of the protected host IP addresses;
- Host Guard group rule: One protected host IP address

The work principle of the Host Guard function is as follows:

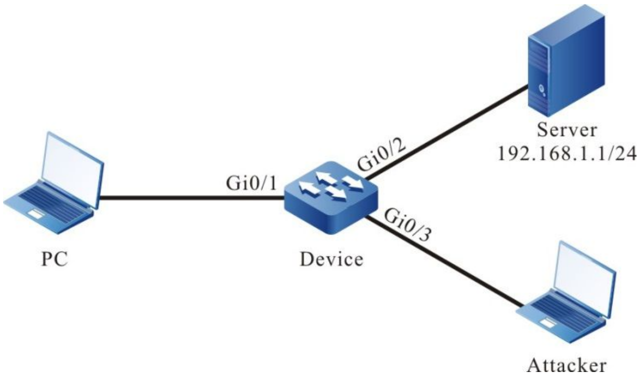


Figure 59–1 The Brief Diagram of the Host Guard Function

As shown in the above figure, Attacker can make use of the IP address 192.168.1.1 of the Server to forge the ARP packet and forward to PC via Device, damaging the ARP table on PC. As a result, PC cannot access Server normally.

On Device, after applying the IP address of Server 192.168.1.1 as one host guard group rule to port gigabitethernet0/2, when the sending IP address in the ARP packet received by Device is the same as the IP address of Server and if the receiving port is gigabitethernet0/2, the packet can be processed normally; if the receiving port is not gigabitethernet0/2, the packet is dropped. That is, the ARP packet sent by Server can only be forwarded via port gigabitethernet0/2. The ARP packet forged by Attacker is dropped.

59.2 Host Guard Function Configuration

Table 59-1 The Configuration List of the Host Guard Function

Configuration Task	
Configure the Host Guard function	Configure the host protect group
	Configure the application of the host protect group

59.2.1 Configure Host Guard Function -B -S -E -A

Configuration Conditions

None

Configure Host Guard Group

Host guard group comprises a series of host guard group rules. We can configure the IP addresses of the gateway and important server in the network as the rules in the host guard group.

Table 59-2 Configure Host Guard Group

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Create the host guard group	**host-guard group** *group-name*	Mandatory By default, do not create any host guard group.
Configure the host guard group rule	**permit host** *ip-address*	Mandatory By default, do not configure host guard group rule.

NOTE

- Each host guard group supports 128 host guard group rules at most.

Configure Application of Host Guard Group

Apply the host guard group to the port. We can monitor the received ARP packets, realizing the protection for the ARP table.

Table 59-3 Configure Application of Host Guard Group

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the application of the host guard group	**host-guard binding** *group-name*	Mandatory By default, there is no applied host guard group on the port or aggregation group.

59.2.2 Monitoring and Maintaining of Host Guard *-B -S -E -A*

Table 59-4 Host Guard Monitoring and Maintaining

Command	Description
show host-guard binding [**interface** *interface-id* | **link-aggregation** *link-aggregation-id*]	Display the application information of the host guard group
show host-guard group [*group-name*]	Display the configuration information of the host guard group and rules

60 AAA

60.1 Overview

AAA refers to Authentication, Authorization, and Accounting. Since the network appeared, Authentication, Authorization, and Accounting mechanism has become the basis of the network operation. The using of the resources in the network needs to be managed by Authentication, Authorization, and Accounting. AAA adopts the client/server architecture. The client runs on NAS (Network Access Server) and the server manages the user information in a centralized manner. For the user, NAS is the server; for the server, NAS is the client.

Authentication means to authenticate the user when using the resources in the network system. During the process, get the ID information by interacting with the user and then submit to the authentication server; the latter checks and processes the ID information with the user information saved in the database, and then confirm whether the user ID is correct according to the processing result. Authorization means that the authorized user of the network system uses its resources by the specified mode. The process specifies the services and authorities that the authenticated user can use and own after being connected to the network, such as the authorized IP address. Accounting means that the network system collects and records the using of the user for the network resources, so as to charge the user for the network using fees, or used for auditing.

RADIUS is one protocol of the C/S architecture. Its client is the NAS server at first. RADIUS protocol authentication mechanism is flexible and can adopt PAP, CHAP or Unix login authentication mode. RADIUS is one expansible protocol and all its work is based on the vector of Attribute-Length-Value. The basic work principle of RADIUS is: The user is connected to NAS; NAS uses Access-Require packet to submit the user information to the RADIUS server, including user name, password, and so on. The user password is encrypted via MD5. The two parties use the share key, which is not spread via the network. RADIUS server checks the validity of the user name and password and provides one Challenge if necessary, requiring the further authentication for the user. We also can perform the similar authentication for NAS. If valid, return the Access-Accept packet to NAS, permitting the user to perform the next work. Otherwise, return the Access-Reject packet, refusing the user access. If permitting the access, NAS initiates the statistics request Account-Require to the RADIUS server. RADIUS server replies Account-Accept, beginning the statistics for the user. Meanwhile, the user can perform its own operations.

TACACS is one old authentication protocol for the Unix network. It permits the remote access server to transit the user login password to the authentication server. The authentication server decides whether the user can log in to the system. TACACS is one encryption protocol, but its security is poorer that TACACS+ and RADIUS. In fact, TACACS+ is one new protocol. TACACS+ and RADIUS replaces the earlier protocol in the present network. TACACS+ uses TCP, while RADIUS uses UDP. RADIUS combines the authentication and authorization from the user aspect, while TACACS+ separates the two operations.

60.2 AAA Function Configuration

Table 60-1 The Configuration List of the AAA Function

Configuration Task	
Configure the AAA basic functions	Enable the AAA function
Configure the AAA authentication function	Configure the login authentication prompt information
	Configure the login authentication method list
	Configure the authentication method list in privileged mode
	Configure the PPP authentication method list
	Configure the connection authentication method list
Configure the AAA authorization function	Configure the command authorization method list
	Configure the SHELL authorization method list
	Configure the network service authorization method list
	Configure enabling the Console authorization
Configure the AAA statistics function	Configure the command statistics method list
	Configure the SHELL statistics method list
	Configure the network service statistics method list
	Configure the system event statistics method list
	Configure the connection statistics method list
	Configure disabling the null user name statistics
	Configure sending the statistics update packet
Configure the RADIUS scheme	Configure the RADIUS server

Configuration Task	
	Configure the RADIUS server group
Configure the TACACS scheme	Configure the TACACS server
	Configure the TACACS server group

60.2.1 Configure AAA Domain *-B -S -E -A*

Domain: (domain) NAS management of users is based on ISP (Internet Service Provider) domain. Each user belongs to an ISP domain. Generally the ISP domain to which a user belongs is determined by the user name provided by the user at times of login. By default, the system has a "system" domain. Methods for authenticating, authorizing, and charging every type of users can be configured in that domain.

A domain-based solution for management of users and AAA is explained in full as follows:

NAS device's management of users is based on ISP domain. Generally, the ISP domain to which a user belong is determined by the user name provided by the user at times of login.

User name entered by user = “device understandable user name” + “domain name”

During user authentication, the Device determines the domain to which the user belongs in the following order and then implements the AAA strategy in the domain:

1) [optional] Authentication domain specified in login/access module configurations;
2) ISP domain specified in user name;
3) System default ISP domain.

Configuration Conditions

None

Configure ISP Domain

Table 60-2 Configure AAA Domain

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter ISP domain view	**domain** *isp-name*	Optional. By default, the system has an ISP domain named "system".

Steps	Command	Description
Exit to global configuration mode	**exit**	-
Configure default ISP domain	**domain default enable** *isp-name*	Optional. By default, the system's default ISP domain is the "system" domain.

60.2.2 Configure AAA Authentication Function *-B -S -E -A*

AAA provides a series of authentication modes to ensure the security of the device and network services. For example, authenticate the user login, preventing the invalid user from operating the device; authenticate the user entering the privilege mode, limiting the using authority of the user for the device; authenticate the PPP session connection, limiting the setup of the invalid connection.

Configuration Conditions

To configure the AAA authentication function, first complete the following configuration:

- Enable the AAA function

Configure Login Authentication Prompt Information

The login authentication prompt information includes the welcome information displayed by the device, authentication failure prompt information, and the prompt information of the user inputting user name and password.

Table 60-3 Configure Login Authentication Prompt Information

Step	**Command**	**Description**
Enter global configuration mode	**configure terminal**	-
Configure the login welcome information	**aaa authentication banner** *banner*	Optional By default, the displayed login welcome information is User Access Verification.
Configure the login failure prompt information	**aaa authentication fail-message** *fail-message*	Optional By default, The login failure prompt information is "Access denied!".

Step	Command	Description
Configure the prompt information when inputting the user name	**aaa authentication username-prompt** *username-prompt*	Optional By default, the prompt information when inputting the user name is "login:".
Configure the prompt information when inputting the password	**aaa authentication password-prompt** *password-prompt*	Optional By default, the prompt information when inputting the password is "password:".

NOTE

- When logging in to the device, the displayed welcome information and login failure prompt information adopt the same characters as the head and end indicating characters. For example, if hoping that the output welcome information displays as “welcome”, the input banner is “^welcome^”. “^” is the head and end indicting character.

Configure Login Authentication Method List

When the user logs in to the device, the device prompts the user to input the user name and password. AAA can use **aaa authentication login** to authenticate the user ID.

Table 60-4 Configure Login Authentication Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the login authentication method list	**aaa authentication login** { **default |** *list-name* } { **none** / **enable** / **local** / **line** / **radius** / **tacacs** / *group-name* }	Optional By default, the login authentication method list is not configured.

NOTE

- When using, it is necessary to use with the **login authentication** command in the line configuration mode, making the method list be used for the user login and ID authentication.

- The **aaa authentication login** command supports configuring four login authentication methods at the same time. After the current method becomes invalid, begin to try another method. The local authentication method does not become invalid forever.
- It is suggested that the user configures multiple methods to authenticate and the last one uses the **none** method. This can ensure that the user still can log in to the device after all methods become invalid.

Configure Privileged Authentication Method List

After the user logs in to the device successfully, AAA can authenticate the user that inputs the enable command to enter the privileged mode, preventing the un-authenticated user from entering the privileged mode.

Table 60-5 Configure Privileged Authentication Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the privileged authentication method list	**aaa authentication enable default** { **none** / **enable** / **line** / **radius** / **tacacs** / *group-name* }	Optional By default, the privileged authentication method list is not configured.

NOTE

- When using the RADIUS authentication method, use the password in the $enabLEVEL$ format as the authentication password. LEVEL indicates the user level the current user enters. The value range is 0-15 and 15 is the highest level.

Configure PPP Authentication Method List

In the PPP environment, when the PPP user wants to set up the session with the peer, the peer can authenticate the connection request of the PPP user via the specified authentication method.

Table 60-6 Configure PPP Authentication Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the PPP authentication method list	**aaa authentication ppp** { **default** | *list-name* } { **none** /	Optional

Step	Command	Description
	local / **radius** / **tacacs** / *group-name* }	By default, the PPP authentication method list is not configured.

NOTE

- When using, it is necessary to configure the **ppp authentication** command in the PPP interface to reference the method list. For the configuration, refer to the PPP configuration manual.

Configure Connection Authentication Method List

In the 802.1x environment, when the 802.1x user wants to set up the session with the peer, the peer can authenticate the connection request of the 802.1x user via the specified authentication method.

Table 60-7 Configure connection Authentication Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the connection authentication method list	**aaa authentication connection** { **default |** *list-name* } { **none** / **local** / **radius** / **tacacs** / *group-name* }	Optional By default, the connection authentication method list is not configured.

60.2.3 Configure AAA Authorization Function *-B -S -E -A*

After authenticating successfully, the AAA authorization function can control the access of the user for the network resources, limiting the user from accessing the un-authorized network resources.

Configuration Conditions

To configure the AAA authorization function, first complete the following configuration:

- Enable the AAA function

Configure Command Authorization Method List

The device has the commands of 0-15 levels. The command authorization is to confirm the command level used by the user via the authorization method, limiting the user from using the command higher than the current level.

Table 60-8 Configure Command Authorization Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the command authorization method list	**aaa authorization commands** *cmd-lvl* { **default |** *list-name* } { **if-authenticated** / **local** / **none** / **radius** / **tacacs** / *group-name* }	Mandatory By default, the command authorization method list is not configured.
Enable the command authorization	**aaa authorization config-commands**	Mandatory By default, the command authorization function is disabled.

NOTE

- When using, it is necessary to use with the **authorization** command in the line configuration mode, making the method list be used for the user login and ID authentication.
- The configurations of the command **aaa authorization commands** and **aaa authorization config-commands** has no order.

Configure SHELL Authorization Method List

After the user logs in to the device, authorize the current user, including the user level, SHELL timeout, the command of level-1 user, and so on.

Table 60-9 Configure SHELL Authorization Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the SHELL authorization command method list	**aaa authorization exec** { **default |** *list-name* } { **if-authenticated** / **local** / **none** / **radius** / **tacacs** / *group-name* }	Mandatory By default, the SHELL authorization command

Step	Command	Description
		method list is not configured.

NOTE

- When using, it is necessary to use with the **authorization** command in the line configuration mode, making the authorization method list be used for the user login and ID authentication.

Configure Network Service Authorization Method List

After configuring the network service authorization method list and when the user runs the network service, perform the authorization to decide the authority of the user using the network service.

Table 60-10 Configure Network Service Authorization Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the network service authorization method list	**aaa authorization network** { **default** | *list-name* } { **if-authenticated** / **local** / **none** / **radius** / **tacacs** / *group-name* }	Mandatory By default, the network service authorization method list is not configured.

NOTE

- When using, it is necessary to reference the authorization method list in the specified network service. Currently, support the PPP and other network protocols.

Configure Enabling Console Authorization

If it is necessary to perform the access limitation for the Console port, we can enable the Console port authorization and then the device uses the SHELL authorization method lost to authorize.

Table 60-11 Configure Enabling Console Authorization

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure enabling the Console authorization	**aaa authorization console**	Mandatory By default, the Console authorization is not enabled.

60.2.4 Configure AAA Accounting Function *-B -S -E -A*

We can adopt the customized method to measure the information about the user using the command on the device, login session, network service status, and system event. The accounting result can serve as the basis of the user accounting.

Configuration Conditions

To configure the AAA accounting function, first complete the following configuration:

- Enable the AAA function

Configure Command Accounting Method List

When the user logs in to the device and operates the command, we can measure the executed commands by configuring the command accounting method list.

Table 60-12 Configure Command Accounting Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the command accounting method list	**aaa accounting commands** *cmd-lvl* { **default** | *list-name* } { **none** | { **start-stop** [**broadcast**] { **tacacs** / *group-name* } } }	Mandatory By default, the command accounting method list is not configured.

NOTE

- When using, it is necessary to use with the **accounting commands** command in the line configuration mode, making the accounting method be applied to the terminal the user logs in.

- Only the TACACS method supports the command accounting.

Configure SHELL Accounting Method List

After logging in to the device, the user can configure the SHELL accounting method to measure the user login information.

Table 60-13 Configure SHELL Accounting Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the SHELL accounting method list	**aaa accounting exec** { **default** | *list-name* } { **none** | { **start-stop** | **stop-only** | **wait-start** [**broadcast**] { **radius** / **tacacs** / *group-name* } } }	Mandatory By default, the SHELL accounting method list is not configured.

NOTE

- To perform the accounting work as little as possible, you can use the key word **stop-only**, sending the stop accounting packet only when the requested user session ends.
- To understand more detailed accounting information, you can use the key word **start-stop** so that the device uses RADIUS or TACACS to send the accounting packet when the requested session starts and the end packet when the session ends.
- To get larger control authority for the accounting, you can use **wait-start** to ensure that the user session request can get permission only after the RADIUS or TACACS server receives the start packet.
- When using, it need to use with the command **accounting exec** in the line configuration mode, making the accounting method list be applied to the terminal the user logs in to.

Configure Network Service Accounting Method List

After logging in to the device, the user can configure the network service accounting method list to measure the network services used by the user (such as PPP).

Table 60-14 Configure Network Service Accounting Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the network service accounting method list	**aaa accounting network** { **default** | *list-name* } { **none** | { **start-stop** | **stop-only** | **wait-start** [**broadcast**] { **radius** / **tacacs** / *group-name* } } }	Mandatory By default, do not measure the network services.

NOTE

- In the PPP environment, it is necessary to use with the **ppp accounting** command in the PPP interface, making the accounting method list be applied to the specified PPP connection.

Configure System Event Accounting Method List

The user can send the system starting and restarting events to the server for accounting by configuring the system event accounting method list.

Table 60-15 Configure the system event accounting method list

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the system event accounting method list	**aaa accounting system default** { **none** | { **start-stop** [**broadcast**] { **tacacs** / *group-name* } } }	Mandatory By default, do not measure the system events.

NOTE

- The system event accounting only supports the TACACS protocol, but does not support the RADIUS protocol.

Configure Connection Accounting Method List

The user can send the 802.1x event to the server for accounting by configuring the connection accounting method list.

Table 60-16 Configure Connection Accounting Method List

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the connection accounting method list	**aaa accounting connection** { **default** | *list-name* } { **none** | { **start-stop** | **stop-only** | **wait-start** [**broadcast**] { **radius** / **tacacs** / *group-name* } } }	Mandatory By default, do not measure the connections.

Configure Disabling Null User Name Accounting

The user can disable the enabled function of measuring the users with null user names by configuring the **aaa accounting suppress null-username** command.

Table 60-17 Configure Disabling Null User Name Accounting

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure disabling the null user name accounting	**aaa accounting suppress null-username**	Mandatory By default, enable the accounting for the null user names

Configure Sending Accounting Update Packets

The user can configure the mode of sending the accounting update packets, including the real-time sending and periodical sending.

Table 60-18 Configure Sending Accounting Update Packets

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure sending the accounting update packets	**aaa accounting update** { **newinfo** | **periodic** *interval* }	Mandatory By default, do not send the accounting update packet.

60.2.5 Configure the Method for Entering Privilege Mode Authentication

-B -S -E -A

After the user has successfully logged on to the device, AAA can authenticate the user when he/she enters enable command to access the privilege mode. If the user fails the authentication, he/she will be denied access to the privilege mode.

Configuration Conditions

None

Configure Privilege Mode Authentication Method

Table 60-19 Configure Privilege Mode Authentication Method

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure privilege mode authentication method	**aaa authentication enable-method** { **none** / **enable** / **radius-group** *group-name* / **tacacs-group** *group-name* }	Optional. By default, configure privilege mode authentication method is enable.

NOTE

- When **RADIUS** authentication is used, the password for a user name in the format of **$enabLEVEL$** will be verified. **LEVEL** denotes the user level that the current user is trying to log in, it is a value in the range of **0-15**, **15** is the highest level.

60.2.6 Configure to Turn on Command Line Authorization ***-B -S -E -A***

Configuration Conditions

None

Configure Enable Command Authorization

Commands available on a Device can be of Level 0~15. Command authorization refers to the process in which the level of the command that the user tries to use is verified by authorization method. The user is restricted from using a command of level higher than the user's current level.

Table 60-20 Enable Command Authorization in Global Mode

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable command authorization	**aaa authorization config-commands**	Required. By default, command authorization function is turned off.

Configure to Enable Console Authorization

When it is necessary to implement restrictions on access to Console Port, CONSOLE Port authorization can be enabled. In such cases, command authorization function also has to be enabled. Once both functions are enabled, the Device will authorize the command to be executed on CONSOLE port by authentication.

Table 60-21 Configure to Enable Console Authorization

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure to enable Console authorization	**aaa authorization console**	Required. By default, Console authorization is not required.

60.2.7 Configure System Event Accounting Function *-B -S -E -A*

Users may send information on such events as system start and restart to server for accounting purpose by configuring a system event accounting method.

Configuration Conditions

None

Configure System Event Statistical Method

Table 60-22 Configure System Event Accounting Method List

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure system event accounting method	**aaa accounting system** { **none** | { **start-stop** [**broadcast**] { **tacacs-group** *group-name* } } }	Required By default, system event accountings are not compiled.

NOTE

- System event accounting function only supports **TACACS** protocol but does not support **RADIUS** protocol.

60.2.8 Configure Accounting Related Attributes *-B -S -E -A*

Configuration Conditions

None

Configure to Turn off Empty User Name Statistics

Users may turn off AAA empty user name accountings by configuring the **aaa accounting suppress null-username** command. By default, empty user name accounting is turned on.

Table 60-23 Configure to Turn off Empty User Name Accounting

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure to turn off empty user name accounting	**aaa accounting suppress null-username**	Required. By default, empty user name accounting is turned on.

Configure to Send Accounting Refresh Message

User can configure the method to send accounting refresh message to either real-time sending or periodical sending.

Table 60-24 Configure to Send Accounting Refresh Message

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure to send accounting refresh message	**aaa accounting update periodic** *interval*	Required. By default, accounting refresh message is not sent.

Configure the Method for Handling Failed Submissions of Accounting

Table 60-25 Configure the Method for Handling Failed Submissions of Accounting

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the method for handling failed submissions of accounting	**aaa accounting start-fail {online | offline}**	Optional. By default, once the submissions of accounting fails, the user will not be able to get online.

60.2.9 Configure RADIUS Scheme *-B -S -E -A*

To configure the RADIUS scheme, you need to complete the configuration of the key parameters of the server/server group.

Configuration Conditions

To configure the RADIUS scheme, first complete the following configuration:

- Enable the AAA function

Configure RADIUS Server

When AAA needs to use RADIUS to perform the authentication, authorization, and statistics, it is necessary to configure the RADIUS server parameters, including server IP address, authentication/authorization port, statistics port, shared key, and so on.

Table 60-26 Configure RADIUS Server

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the RADIUS server	**radius-server host** *ip-address* [**acc-port** *acc-port-num*] [**auth-port** *auth-port-num*] [**priority** *priority*] [**key** [**0** | **7**] *key*]	Mandatory By default, the RADIUS server is not configured.
Configure the RADIUS dead time	**radius-server dead-time** *dead-time*	Optional By default, the dead time of the RADIUS server is 0.
Configure the RADIUS shared key	**radius-server key** [**0** | **7**] *key*	Optional By default, the RADIUS encrypted key is not configured.
Configure the maximum re-transmission times of RADIUS	**radius-server retransmit** *retries*	Optional By default, the maximum time of re-transmitting to the RADIUS server is 3.
Configure the response timeout of the RADIUS server	**radius-server timeout** *timeout*	Optional By default, the timeout of waiting for the RADIUS server response is 5s.
Configure the selected interface of the RADIUS source address	**ip radius source-interface** *interface-name* [**vrf** *vrf-name*]	Optional By default, the source interface of interacting with the RADIUS

Step	Command	Description
		server is not configured.
Configure not to check the tag identifier when parsing the tunnel property sent by the RADIUS server	**radius-server tunnel without-tag**	Optional By default, the tag identifier is required when parsing the tunnel property sent by the RADIUS server.
Configure the value of the service-type property in the login authentication RADIUS packet	**radius login service-type** *attr-value*	Optional By default the service-type value in the RADIUS packet is 7.

NOTE

- We can execute the **radius-server host** command for many times to configure multiple RADIUS servers. The device selects the server to authenticate according to the configuration order. After one server fails, the device automatically selects the next server.
- The device selects the order of using the RADIUS server according to the configured priority value.
- The dead time means: The device remarks the RADIUS server that does not answer the authentication request as unavailable and does not send request during the dead time.
- The configured share keys on the device and the RADIUS server should be consistent.

Configure RADIUS Server Group

Configure the RADIUS server group. When configuring the method list, reference the server group name and then you can use the RADIUS server group to authenticate, authorize and measure the user.

Table 60-27 Configure RADIUS Server Group

Step	Command	Description
Enter global configuration mode	**configure terminal**	-

Step	Command	Description
Configure the RADIUS server group name	**aaa group server radius** *group-name*	Mandatory By default, the RADIUS server group name is not configured.
Configure adding the global server to the server group	**server** *ip-address* [**auth-port** auth-*port-num*] [**acct-port** acct-*port-num*]	Optional By default, the global server is not added to the server group.
Configure the private RADIUS server	**server-private** *ip-address* [**acc-port** *acc-port-num*] [**auth-port** *auth-port-num*] [**key** [**0** | **7**] *key*] [**priority** *priority*]	Optional By default, the private RADIUS server is not configured.
Configure the VRF attribute of the RADIUS server group	**ip vrf forwarding** *vrf-name*	Optional By default, the VRF attribute of the RADIUS server group is not configured.

NOTE

- When configuring the RADIUS server group name, there should be as clear meaning as possible and avoid using the key words that may cause confusion. For example, tac, rad, and loc may be confused with **tacacs**, **radius**, and **local** when configuring the method list.
- The private server is completely independent from the global configured server, so it can be the same as the global configured server.
- Select at least one of private server and global server to configure.

60.2.10 Configure TACACS Scheme *-B -S -E -A*

To configure the TACACS scheme, we need to configure the key parameters of the server/server group.

Configuration Conditions

To configure the TACACS scheme, first complete the following configuration:

- Enable the AAA function

Configure TACACS Server

After configuring the TACACS server and if AAA needs to use the TACACS method to authenticate, authorize, and measure, we need to configure the parameters of the TACACS server, including the server IP address, share key, server port number and so on.

Table 60-28 Configure the TACACS Server

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the TACACS server	**tacacs-server host** *ip-address* [**key** [**0** | **7**] *key*] [**priority** *priority*] [**port** *port-num*] [**timeout** *timeout*]	Mandatory By default, the TACACS server is not configured.
Configure the TACACS share key	**tacacs-server key** [**0** | **7**] *key*	Optional By default, the TACACS share key is not configured.
Configure the timeout of the TACACS server response	**tacacs-server timeout** *timeout*	Optional By default, the timeout of waiting for the answer of the TACACS server is 5s.
Configure the interface selected by the TACACS source address	**ip tacacs source-interface** *interface-name* [**vrf** *vrf-name*]	Optional By default, the source interface interacting with the TACACS server is not configured.

NOTE

- We can execute the **tacacs-server host** command for many times to configure multiple TACACS servers. The device selects the server to authenticate according to the configuration order. After one server fails, the device automatically selects the next server.

- The configured share keys on the device and the TACACS server should be consistent.

Configure TACACS Server Group

Configure the TACACS server group. When configuring the method list, reference the server group name and then you can use the TACACS server group to authenticate, authorize and measure the user.

Table 60-29 Configure the TACACS Server Group

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the TACACS server group name	**aaa group server tacacs** *group-name*	Mandatory By default, the TACACS server group name is not configured.
Configure adding the global server to the server group	**server** *ip-address*	Optional By default, the TACACS server group member is not configured.
Configure the private TACACS server	**server-private** *ip-address* [**timeout** *timeout*] [**port** *port-num*] [**key** [**0** | **7**] *key*] [**priority** *priority*]	Optional By default, the private TACACS server is not configured.
Configure the VRF attribute of the TACACS server group	**ip vrf forwarding** *vrf-name*	Optional By default, the VRF attribute of the TACACS server group is not configured.

NOTE

- When configuring the TACACS server group name, there should be as clear meaning as possible and avoid using the key words that may cause confusion. For example, tac, rad, and loc may be confused with **tacacs**, **radius**, and **local** when configuring the method list.

- The private server is completely independent from the global configured server, so it can be the same as the global configured server.

60.2.11 AAA Monitoring and Maintaining *-B -S -E -A*

Table 60-30 AAA Monitoring and Maintaining

Command	Description
show aaa	Display the AAA basic information
show aaa configure	Display the AAA configuration information
show aaa module	Display the AAA function module and the result of the module operating AAA at last
show aaa server [**radius** | **tacacs**]	Display the RADIUS/TACACS server configuration and status of AAA
show aaa session	Display the AAA statistics session
show aaa source-address	Display the source address used by AAA

60.3 AAA Typical Configuration Example

60.3.1 Configure Telnet User Login to Use Local Authentication *-B -S -E -A*

Network Requirements

1. Configure Device to use local authentication for Telnet user login

Network Topology

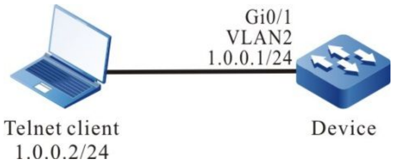


Figure 60-1 Networking of Configuring Telnet User Login to Use Local Authentication

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Configure Device.

#Configure the user name as admin and password as admin.

```
Device#configure terminal
Device(config)#user admin password 0 admin
```

#Configure the AAA authentication/authorization as local authentication.

```
Device(config)#aaa new-model
Device(config)#aaa authentication login default local
```

#Configure the Telnet session and enable the AAA local authentication.

```
Device(config)#line vty 0 15
Device(config-line)#login authentication default
Device(config-line)#exit
```

Step 4: Check the result.

When Telnet client logs in to Device, input the user name admin and password admin according to the prompt, and then log in to the Shell user interface of Device successfully.

60.3.2 Configure Telnet User Login to Use RADIUS Authentication/Authorization and Accounting *-B -S -E -A*

Network Requirements

1. Device is connected to the Telnet and RADIUS server and the IP route is available.
2. The IP address of the RADIUS server is 2.0.0.2/24, the authentication/authorization port is 1812, the statistics port is 1813, and the share key is admin.
3. When Telnet user logs into Device, it is required to authenticate/authorize and measure via the RADIUS server.
4. When the RADIUS server fails, use the local authentication and authorization.

Network Topology

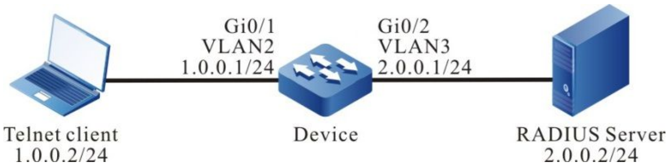


Figure 60-2 Networking of Configuring Telnet User Login to Use RADIUS Authentication/Authorization and Accounting

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Configure Device.

#Configure AAA and use the RADIUS authentication/authorization and accounting.

NOTE

- Authentication and authorization first use the first method in the method list; when the server fails, use the second method to authenticate and authorize.

```
Device(config)#aaa new-model
Device(config)#aaa authentication login authen-list radius local
Device(config)#aaa authorization exec author-list radius local
Device(config)#aaa accounting exec account-list start-stop radius
```

#Configure RADIUS server, authentication port as 1812, statistics port as 1813 and share key as admin.

```
Device(config)#radius-server host 2.0.0.2 auth-port 1812 acct-port 1813 key admin
```

#Configure the Telnet session and enable the RADIUS authentication/authorization and accounting.

```
Device(config)#line vty 0 15
Device(config-line)#login authentication authen-list
Device(config-line)#authorization exec author-list
Device(config-line)#accounting exec account-list
Device(config-line)#exit
```

Step 4: Configure the RADIUS server.

For the interface setting of the RADIUS server, refer to the help document of the server. The following lists the main steps.

#Add the user admin on the RADIUS server, set the password as admin and configure the user label as 15.

#Set the IP address of the server as 2.0.0.2, share key as admin, authentication port as 1812 and accounting port as 1813.

#Set the IP address of the client as 2.0.0.1 and the share key as admin.

Step 5: Check the result, and verify the authentication/authorization and accounting.

#After Telnet user logs in to Device, authorize successfully, and use the **show privilege** command to view the user priority 15.

#We can view the login and disconnection statistics information on the RADIUS server.

60.3.3 Configure Telnet User Level Switching to Use RADIUS Authentication

-B -S -E -A

Network Requirements

1. Device is connected to the Telnet and RADIUS server and the IP route is available.
2. The IP address of the RADIUS server is 2.0.0.2/24, the authentication/authorization port is 1812, and the share key is admin.
3. When the user level switches from 1 to 3 after Telnet user logs in to Device, it is required to authenticate via RADIUS server.

Network Topology

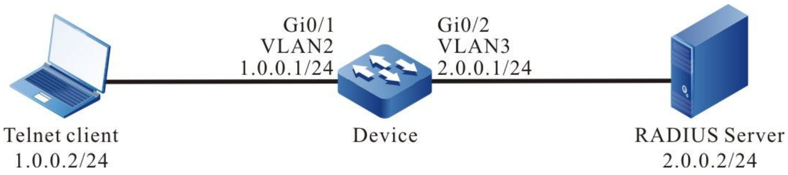


Figure 60-3 Networking of Configuring Telnet User Level Switching to Use RADIUS Authentication

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Configure Device.

#Configure the user level switching to use the RADIUS authentication.

```
Device(config)#aaa new-model
Device(config)#aaa authentication enable default radius
```

#Configure the RADIUS server, authentication port as 1812 and share key as admin.

```
Device(config)#radius-server host 2.0.0.2 auth-port 1812 acct-port 1813 key admin
```

Step 4: Configure the RADIUS server.

For the interface setting of the RADIUS server, refer to the help document of the server. The following lists the main steps.

#Add the user name $enab3$ with user level 3 and set the password as admin.

NOTE

- User level switching is fixed to use the user name in the format of $enabLEVEL$ for authentication. LEVEL is the level that the user wants to switch to.
- When the user level is reduced, do not need authentication.

Step 5: Check the result.

After Telnet user inputs the user name and password to log in according to the prompt, the user level is 1 by default. After executing the command enable 3, input the password admin. After being authenticated by RADIUS server successfully, the user level is switched to 3.

60.3.4 Configure TACACS Authorization and Accounting of Shell Command

-B -S -E -A

Network Requirements

1. Device is connected to the Telnet and RADIUS server and the IP route is available.
2. The IP address of the RADIUS server is 2.0.0.2/24, the service port is 49, and the share key is admin.
3. After Telnet client logs in to Device, the operated shell command with user level 15 is required to be authorized via TACACS server and record the shell command to the TACACS server.

Network Topology

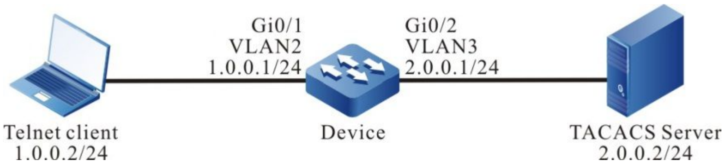


Figure 60–4 Networking of Configuring the TACACS Authorization and Accounting of the Shell Command

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Configure Device.

#Configure the TACACS command authorization and accounting.

NOTE

- Before authorization and accounting, the authentication should be successful.

```
Device(config)#aaa new-model
Device(config)#aaa authentication login shell tacacs
Device(config)#aaa authorization commands 15 cmd-author tacacs
Device(config)#aaa authorization config-commands
Device(config)#aaa accounting commands 15 cmd-accounting start-stop tacacs
```

#Configure the TACACS server, the service port is 49, and the share key is admin.

```
Device(config)#tacacs-server host 2.0.0.2 port 49 key admin
```

#Configure the Telnet session and enable the TACACS authorization and accounting.

```
Device(config)#line vty 0 15
Device(config-line)#login authentication shell
Device(config-line)#authorization commands 15 cmd-author
Device(config-line)#accounting commands 15 cmd-accounting
Device(config-line)#exit
```

Step 4: Configure the TACACS server.

For the interface setting of the TACACS server, refer to the help document of the server. The following lists the main steps.

#Add the client 2.0.0.1 on the server, the share key is admin, and select “TACACS+(Cisco IOS)” authentication.

#Set the Shell command authorization for Telnet user admin. Permit the commands **configure terminal**, **router ospf** and **router rip**, and refuse the other commands.

Step 5: Check the result.

#After Telnet user logs in to Device, execute the Shell command. The authorized command can be executed successfully and the un-authorized command authorization failed.

```
Device#configure terminal
% Enter configuration commands, one per line.  End with CNTL+Z.
Device(config)#router ospf 100
Device(config-ospf)#exit
Device(config)#router rip
Device(config-rip)#exit
Device(config)#interface gigabitethernet 0/1
Command authorization failed
Device(config)#router bgp 100
Command authorization failed
```

#View the Shell command accounting information.

On the TACACS server, we can see the accounting information of the Shell command.

61 802.1X

61.1 Overview

61.1.1 802.1X -B -S -E -A

802.1X is a broadband access authentication solution put forward by IEEE in June, 2001. It defines the Port-Based Network Access Control. By utilizing LAN's physical access features of IEEE 802 LAN, 802.1X provides a set of methods for authenticating and authorizing devices access connected to LAN ports via point-to-point.

The 802.1X system is the typical client/server structure, as shown in the following figure, including three entities: Supplicant system (client), Authentication system (authentication device), and Authentication server system (authentication server).

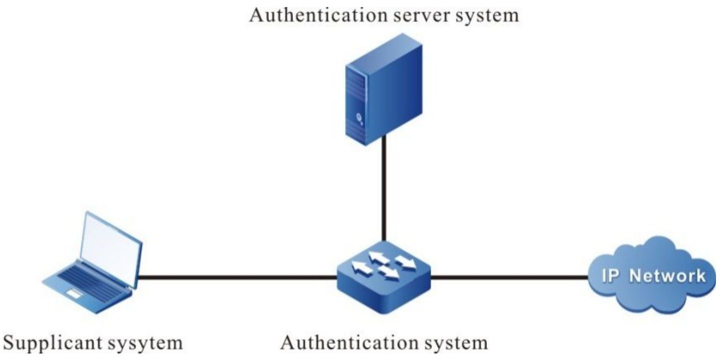


Figure 61-1 802.1X System Architecture

- The client installation supports the client software of the 802.1X authentication, sending the authentication request to the authentication device. If authenticating successfully, connect to the network normally.
- The authentication device is between the client and the authentication server, controlling the network access of the client by interacting with the server.
- Usually, the authentication server is the RADIUS (Remote Authentication Dial-In User Service) server, used to verify the validity of the client and inform the authentication result to the authentication device. The authentication device controls the network access of the client according to the authentication result.

EAP (Extensible Authentication Protocol) used by the 802.1X authentication is one general protocol of the PPP authentication, used to interact the authentication information among the client, authentication device and authentication server. The 802.1X protocol uses EAPOL (EAP Over LAN) frame encapsulation format to encapsulate the EAP packet, realizing the interacting between the client and the authentication device. According to the different application scenarios, the 802.1X protocol encapsulates the EAP packet in the different frame formats, realizing the interacting between the authentication device and the authentication server. In the relay authentication mode, the EAP packet is encapsulated in the EAPOR (EAP Over RADIUS) frame format; in the terminating authentication mode, the EAP packet is encapsulated in the standard RADIUS frame format.

The 802.1X authentication mode includes relay authentication mode and terminating authentication mode.

The relay authentication flow is as follows:

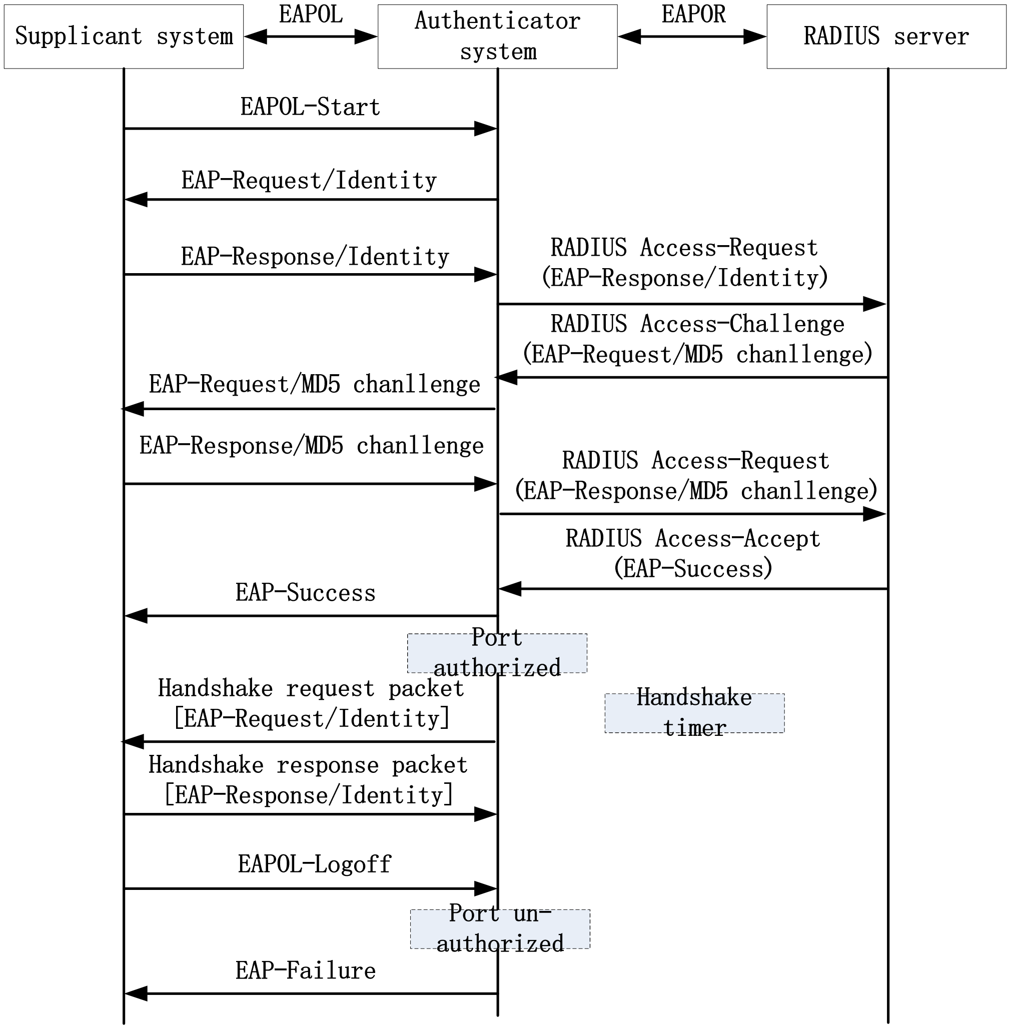

Supplicant system
EAPOL
Authenticator system
EAPOR
RADIUS server
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
RADIUS Access-Request (EAP-Response/Identity)
RADIUS Access-Challenge (EAP-Request/MD5 chanllenge)
EAP-Request/MD5 chanllenge
EAP-Response/MD5 chanllenge
RADIUS Access-Request (EAP-Response/MD5 chanllenge)
RADIUS Access-Accept (EAP-Success)
EAP-Success
Port authorized
Handshake request packet [EAP-Request/Identity]
Handshake timer
Handshake response packet [EAP-Response/Identity]
EAPOL-Logoff
Port un-authorized
EAP-Failure

Figure 61–2 802.1X Relay Authentication Flow

The relay authentication flow is as follows:

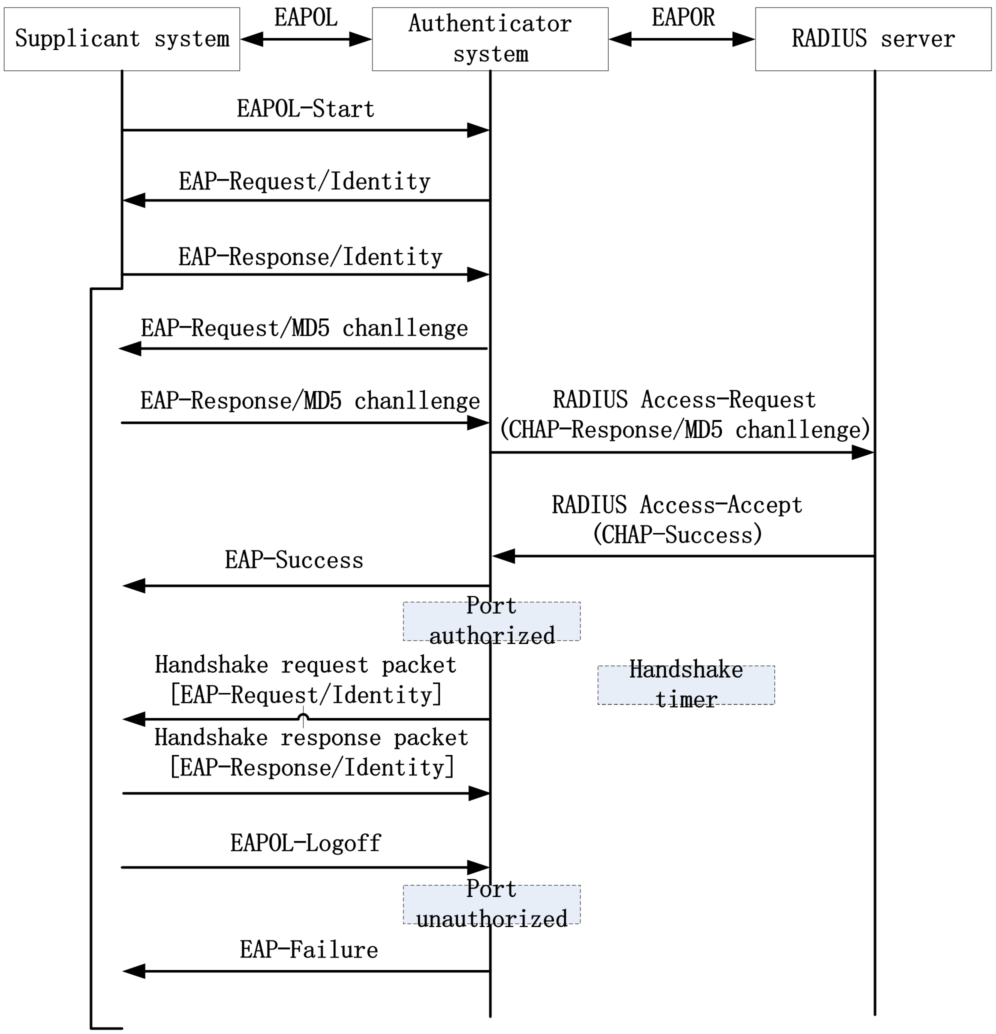
- When the user has the network access requirement, enable the 802.1X client program, input the valid user name and password registered on the authentication server, and initiate the authentication request (EAPOL-Start packet). Here, the client program sends the request authentication packet to the authentication device and starts one authentication process.
- After the authentication device receives the data frame of requesting authentication, send one request frame (EAP-Request/Identity packet) to request the user client program to send the input user name.
- The client program answers the request sent by the authentication device, sending the user name information to the authentication device via the data frame (EAP-Response/Identity packet). The authentication device encapsulates the data frame sent by the client in the packet (RADIUS Access-Request packet) and sends to the authentication server for processing.
- After the RADIUS server receives the user name information forwarded by the

authentication device, compare the information with the user name table in the database, find the corresponding information of the user name, and use one randomly-generated encrypting word to encrypt it. Meanwhile, send the encrypted word to the authentication device via the RADIUS Access-Challenge packet; the authentication device forwards it to the client program.

- After the client program receives the encrypted word forwarded by the authentication device (EAP-Request/MD5 Challenge packet), use the encrypted word to encrypt the password (the encryption algorithm is irreversible, generating the EAP-Response/MD5 Challenge packet), and forward to the authentication server via the authentication device.
- RADIUS authentication server compares the received encrypted password information (RADIUS Access-Request packet) with the local encrypted password information. If they are the same, regard the user as valid user and feed back the message of passing the authentication (RADIUS Access-Accept packet and EAP-Success packet);
- After the authentication device receives the message of passing the authentication, change the port to the authorized state, permitting the user to access the network via the port.
- The client also can send the EAPOL-Logoff packet to the authentication device, actively requesting offline. The authentication device changes the port status from authorized to un-authorized, and sends the EAP-Failure packet to the client.

The authentication needs the authentication device and authentication server to support the EAP protocol.

The terminating authentication flow is as follows:



Supplicant system
EAPOL
Authenticator system
EAPOR
RADIUS server
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
EAP-Request/MD5 chanllenge
EAP-Response/MD5 chanllenge
RADIUS Access-Request (CHAP-Response/MD5 chanllenge)
RADIUS Access-Accept (CHAP-Success)
EAP-Success
Port authorized
Handshake request packet [EAP-Request/Identity]
Handshake timer
Handshake response packet [EAP-Response/Identity]
EAPOL-Logoff
Port unauthorized
EAP-Failure

Figure 61-3 802.1X Terminating Authentication Flow

- The difference between the terminating authentication mode and relay authentication mode is: The random encrypting word used to encrypt the user password information is generated by the authentication device. And the authentication device sends the user name, random-encrypting word and password information encrypted by the client to the RADIUS server for authentication.

The terminating authentication mode is used by the authentication server that is deployed earlier and does not support the EAP protocol.

The authentication device supports two access control modes:

- Port-based access control mode (Portbased): After the first user in the port is authenticated successfully, the other access users can access the network without authentication, but after the first user gets offline, the other users also are refused to access the network.
- User-based access control mode (Macbased): All access users in the port need to be authenticated separately. After one user gets offline, only the user cannot access the network and the other users still can access the network.

Auto VLAN is also called Assigned VLAN. When the client passes the server authentication, the server delivers the authorized VLAN information to the authentication device. If the delivered VLAN exists on the authentication device and is valid, the authentication port is added to the delivered VLAN. After the client gets offline, the port restores to the un-authorized state. The port is deleted from the Auto VLAN and the default VLAN of the port restores to the previous configured VLAN.

After enabling Guest VLAN, the user also can and only can access the resources in the VLAN without authentication. After the user is authenticated successfully, the port leaves Guest VLAN and the user can access other network resources. Usually, the user can get the 802.1X client software in Guest VLAN to upgrade the client, or execute other application program (such as anti-virus software, operation system patch) upgrade. After enabling the 802.1X authentication and configuring Guest VLAN correctly, the port is added to Guest VLAN in Untagged mode. Here, the user in the port of Guest VLAN initiates authentication. If the authentication fails, the port is still in Guest VLAN; if the authentication succeeded, there are two cases:

- If the authentication server delivers one VLAN, the port leaves Guest VLAN and is added to the delivered VLAN. After the user gets offline, the port returns to Guest VLAN.
- If the authentication server does not deliver VLAN, the port leaves Guest VLAN and is added to the configured Config VLAN in the authentication device. After the user gets offline, the port returns to Guest VLAN.

61.1.2 Secure Channel Authentication *-B -S -E -A*

Based on the 802.1X authentication function, the secure channel authentication function can achieve both the 802.1X authentication and pioneer a secure channel for the specified end users. Thus, the end user can visit the resources in the specified network in the unauthentication mode or specify an end user to visit the network resources without authentication.

61.1.3 MAC Address Authentication *-B -S -E -A*

In the actual network, besides lots of end users, there may be some network terminals (such as network printer). The terminals do not carry or cannot install the 802.1X authentication client software and can use the free-client authentication mode to access the network. The authentication method does not need the user to install any 802.1X authentication client software. After the authentication device detects the MAC address of the user for the first time, the authentication device uses the configured user name and password or the user MAC address as the user name and password to send to the authentication server for authentication.

The user name and password format used by the MAC address authentication has two cases:

The MAC address serves as user name and password: Use the MAC address of the authenticated user as the user name and password;

Fixed user name and password: Use the configured user name and password on the authentication device.

61.2 802.1X Function Configuration

Table 61–1 802.1X Function Configuration List

Configuration Task	
Configure the 802.1X authentication function	Enable the 802.1X authentication
Configure the secure channel authentication	Enable the secure channel authentication function
	Configure and apply the secure channel
Configure the 802.1X authentication and secure channel authentication property	Configure the port authentication mode
	Configure the multicast triggering function
	Configure the re-authentication function
	Configure the maximum authentication failure times of the port
	Configure function of omitting the IP field in the user name
	Configure the packet transparent-transmission function
	Configure the keepalive function
	Configure the ARP keepalive function
	Configure the EAPOU function
	Configure the function of not waiting for the server response
Configure the MAC address authentication	Enable the MAC address authentication function
	Configure the MAC address authentication user name format
Configure the public attributes	Configure the log record function of the authentication failure
	Configure the maximum users of the port
	Configure the IP ACL prefix name

Configuration Task	
	Configure the default valid VLAN
	Configure the unauthenticated user to communicate in the VLAN which the PVID locates in
	Configure the port access control mode
	Configure Guest VLAN
	Configure Guest ACL
	Configure the timer parameters
	Restore the default configuration of the port
	Configure the log recording step

61.2.1 Configure 802.1X Authentication Function *-B -S -E -A*

The 802.1X authentication and the MAC address authentication are allowed to be configured simultaneously on the same interface.

- If the authentication is successful when the end user first performs the MAC address authentication, the 802.1X authentication initiated by the end user will not be processed. Otherwise, the 802.1X authentication initiated by the end user will be processed normally.
- When the end user first initiates the 802.1X authentication, then do not perform the MAC address authentication.

Configuration Conditions

None

Enable 802.1X Authentication

To enable the 802.1X authentication function, the end user needs to install the client software with the 802.1X authentication function.

Table 61–2 Enable 802.1X

Step	Command	Description
Enter global configuration mode	**configure terminal**	-

Step	Command	Description
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the 802.1X authentication	**dot1x port-control** { **enable** | **disable** }	Mandatory By default, the 802.1X authentication function in the port is disabled.

NOTE

- To ensure that the functions do not conflict with each other, avoid enabling the 802.1X authentication and interface security function simultaneously on one interface. Do not enable the 802.1X authentication function and security cahnnel authentication function simultaneously on one interface.
- Do not enable the 802.1X authentication function and secure channel authentication function simultaneously on one interface.

61.2.2 Configure Secure Channel Authentication *-B -S -E -A*

Configuration Conditions

None

Enable Secure Channel Authentication

Based on the 802.1X authentication function, the secure channel authentication function can achieve both the 802.1X authentication and pioneer a secure channel for the specified end users. Thus, the end user can visit the resources in the specified network in the unauthentication mode or specify an end user to visit the network resources without authentication.

Table 61–3 Enable Secure Channel Authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration can only take effect on the current interface. After entering the aggregation group configuration mode, the subsequent configuration can only take effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the secure channel authentication	**dot1x free-ip**	Mandatory By default, the secure channel authentication function under the interface is disabled.

NOTE

- To ensure that the functions do not conflict with each other, avoid enabling secure channel authentication function and interface security function simultaneously on one interface.
- Do not enable the 802.1X authentication function and secure channel authentication function simultaneously on one interface.
- Do not enable the MAC address authentication function and the secure channel authentication function simultaneously on one interface.
- When the secure channel authentication function is enabled under the interface but the secure channel rule is not applied or the secure channle rule is not configured, the secure channel authentication function adn the 802.1X authentication function is identical.
- During the secure channel authentication, when the user authentication succeeds, it will occupy the chip resources. If the chip resources are insufficient, it will cause user authentication failure.

61.2.3 Configure 802.1X Authentication and Secure Channel Authentication Property

-B -S -E -A

If the 802.1X authentication function or the secure channel authentication function is not enabled on the interface, then the conifgured related property does not take effect.

Configure Port Authentication Mode

The 802.1X authentication mode includes relay authentication mode and terminating authentication mode.

802.1X authentication system comprises client, authentication device and authentication server. The standard 802.1X protocol defines that the client and authentication server interact via the EAP packet. The authentication device plays as the “relay” role during the interacting. The authentication device encapsulates the EAP data sent by the client in the other protocol, such as the RADIUS protocol, and send to the authentication server. Similarly, the authentication device encapsulates the EAP data sent by the authentication server in the EAPOL packet and forwards to the client. The interacting mode is called relay authentication mode. The relay authentication mode requires that the authentication server supports the EAP protocol. Configuring the authentication mechanism supported by the EAP relay authentication mode depends on the client and authentication server.

The earlier deployed authentication server may not support the EAP protocol and needs to be configured as the terminating authentication mode. The EAP packet of the client is not directly sent to the authentication server, but the authentication device completes the EAP packet interacting with the client. After getting the enough user authentication information, the authentication device sends the authentication information to the authentication server for authentication.

EAP terminating authentication mode supports PAP (Password Authentication Protocol) authentication and CHAP (Challenge Handshake Authentication Protocol) authentication.

Table 61-4 Configure Port Authentication Mode

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the port authentication mode	**dot1x eap-relay** { **enable** | **disable** }	Mandatory By default, the authentication mode in the port is the terminating authentication mode.

NOTE

- Configuring terminating authentication mode only supports the MD5-based (Message Digest Algorithm) EAP authentication. The 802.1x authentication function and secure channel authentication function support the relay and terminating authentication mode.
- The MAC address authentication can only support the terminating authentication mode.

Configure Multicast Triggering Function

Some terminal is installed with the 802.1X authentication client, but the client does not actively initiates the authentication. The authentication process can only depend on the authentication device to trigger. The authentication device periodically sends the multicast packet requesting the user name to the port configured with the multicast triggering. After receiving the packet, the client answers the authentication request of the authentication device and starts the 802.1X authentication.

Table 61–5 Configure Multicast Triggering Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the multicast trigger	**dot1x multicast-trigger**	Mandatory

Step	Command	Description
		By default, the multicast trigger function in the port is disabled.
Configure the triggering period of the multicast	**dot1x multicast-period** *multicast-period-value*	Optional By default, the multicast trigger time in the port is 15s.

NOTE

- If the client does not support the multicast trigger function, the adapter display of the client may be abnormal. Meanwhile, it may cause the re-authentication failure.

Configure Re-authentication Function

To check whether the client is online, avoid the abnormal crashing of the client affecting the correctness of the user accounting, and prevent the client from being used by others, the authentication device periodically initiates the re-authentication request to the client. During the process, the user does not need to input the user name or password again.

Table 61-6 Configure Re-authentication Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the re-authentication	**dot1x reauthentication**	Mandatory

Step	Command	Description
		By default, the re-authentication function is enabled in the port.

Configure Maximum Authentication Failure Times

After the client authentication failure times reach the threshold, the client enters the dead state. During the dead time, the authentication device does not answer the authentication request initiated by the client any more.

Table 61–7 Configure Maximum Authentication Failure Times

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation link-aggregation-id**	
Configure the maximum port authentication failure times	**dot1x max-authfail** *max-authfail-value*	Mandatory By default, the maximum authentication failure time of the port is 1.

Configure to Omit IP Field in User Name

Some 802.1X authentication clients can configure to upload the IP address property and load the IP address before the user name and then send them to the server for authentication. When the IP address of the end user contains 0, for example, the user IP address 192.168.0.1, it may cause authentication failure. In this case, you can configure to omit the IP field in the user name to avoid such problem. After this function is configured, when the user name in the authentication packet carries the IP address which contains 0, the device will omit the IP address contained in the user name of the packet to ensure normal authentication.

Table 61-8 Configure to Omit IP Field in User Name

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to omit the IP field in the user name	**dot1x ignore user-name-ip**	Mandatory By default, the function of omitting the IP field in the user name is disabled.

Configure Packet Transparent Transmission Function

In the actual application environment, the authentication terminal and authentication device may cross the intermediate device. If the intermediate device cannot transmit the EAPOL packet transparently, the authentication cannot be performed normally. To make the authentication be done normally, we need to enable the function of transmitting the EAPOL packet transparently on the port of the intermediate device receiving the EAPOL packet and configure one uplink port for the port. If the port enabled with the function of transmitting the EAPOL packet transparently receives the EAPOL packet, send the packet from the configured uplink port. If the device directly connected to the uplink port is authentication device, the authentication device processes after receiving the EAPOL packet.

Table 61–9 Configure Packet Transparent Transmission Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the packet transparent transmission function	**dot1x eapol-relay** { **enable** | **disble** }	Mandatory By default, the function of transmitting the packet transparently in the port is disabled.

Step	Command	Description
Configure the uplink port	**dot1x eapol-relay uplink** { **interface** *interface-name* **| link-aggregation** *link-aggregation-id* }	Mandatory By default, the port is not configured with the uplink port.

Configure Keepalive Function

To detect whether the client is online, the authentication device periodically sends the EAP-Request/Identity packet to the client. If receiving the EAP-Response/Identity packet from the client, send the EAP-Request/MD5 Challenge packet to the client. If the authentication system receives the EAP-Response/MD5 Challenge packet, confirm that the client is online normally and send the EAP-Success packet to inform the client of keepalive success.

Table 61–10 Configure Keepalive Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the keepalive function	**dot1x keepalive** { **enable | disable** }	Mandatory By default, the keepalive function in the port is disabled.
Configure the keepalive time	**dot1x keepalive period** *period-value*	Optional By default, the keepalive period in the port is 60s.
Configure the times of re-transmitting the keepalive packet	**dot1x keepalive retries** *retries-value*	Optional

Step	Command	Description
		By default, the maximum keepalive time in the port is 3.

NOTE

- The keepalive function needs to be supported by the 802.1X authentication client software (such as MTS TC client). If the client does not support, it may result in the keepalive failure and the user gets offline.

Configure ARP Keepalive Function

To detect whether the client is online after passing the end user authentication, the authentication device sends the ARP request packet to the authenticated user. The authentication device confirms whether the user is online by whether the ARP response packet of the user can be received.

Table 61-11 Configure ARP Keepalive Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the ARP keepalive function	**dot1x client-probe** { **enable** | **disable** }	Mandatory By default, the ARP keepalive function in the port is disabled.
Configure the ARP keepalive period	**dot1x client-probe period** *period-value*	Optional By default, the ARP keepalive period is 60s.

NOTE

- The authentication device must obtain the authenticated IP address of the use to normally trigger the ARP keepalive function.

Configure EAPOU Function

EAPOU is the EAP over UDP protocol. In the standard 802.1X function, the client and authentication device interact with each other via the EAPOL (EAP over LAN) packet. In the actual application environment, because of the network complexity, the terminal to be authenticated (client) and the authentication device may cross the intermediate device. If the intermediate device does not transmit the EAPOL packet transparently, the authentication cannot be performed normally. Enabling the EAPOU function can make the authentication packet (EAP packet) cross the intermediate device, the EAPOU packet is not limited by the intermediate device, and the intermediate device forwards the packet as the general packet, realizing the across-device authentication.

To enable the EAPOU function, we need to configure one interface address on the authentication device, used to receive the EAPOU packet sent by the client. Before sending the EAPOU packet, the client needs to specify the interface address of the authentication device so that the EAPOU packet can be forwarded to the authentication device correctly; after the authentication device receives the EAPOU packet, extract the EAP content from the packet, and then encapsulate as the EAPOR packet and send to the authentication server for authentication. The subsequent process is consistent with the EAPOL authentication mode.

Table 61-12 Configure EAPOU Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the EAPOU function	**dot1x eapou layer2**	Mandatory

Step	Command	Description
		By default, the EAPOU function in the port is disabled.
Configure the UDP port used by the EAPOU function	**dot1x eapou udp-port** *udp-port-value*	Optional By default, the UDP protocol port number used by the EAPOU function is 5651.

NOTE

- To configure the EAPOU function, both the client and authentication device need to support the EAPOU protocol.

Configure Not Waiting for Server Response

In the relay authentication mode, the client may send some packets that the server does not answer. The packets make the session channel between the authentication device and the authentication server be occupied and as a result, the subsequent client authentication fails. We can enable the function of not waiting for the server response in the port to avoid the problem.

Table 61-13 Configure the Function of Not Waiting for the Server Response

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the function of not waiting for the server response	**dot1x nowait-result**	Mandatory By default, the function of not waiting for the server response is disabled.

61.2.4 Configure MAC Address Authentication *-B -S -E -A*

The 802.1X authentication and MAC address authentication are allowed to be configured simultaneously on the same interface.

- If the authentication is successful when the end user first performs the MAC address authentication, the 802.1X authentication initiated by the end user will not be processed. Otherwise, the 802.1X authentication initiated by the end user will be processed normally.
- When the end user first initiates the 802.1X authentication, then do not perform the MAC address authentication.

Configuration Conditions

None

Enable MAC Address Authentication Function

The MAC address authentication is also called free-client authentication. The authentication mode is applicable to the terminal that cannot install the client software for authentication, and also applicable to the end user that does not install client software, but can authenticate without inputting the user name and password.

When configuring the parameters of the MAC address authentication in the authentication device port and if the port does not enable the MAC address authentication function, the configured function does not take effect.

Table 61-14 Enable MAC Address Authentication Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enable the MAC address authentication function	**dot1x mac-authentication** { **enable** | **disable** }	Mandatory By default, the MAC address authentication function in the port is disabled.

NOTE

- To ensure that the functions do not conflict with each other, avoid enabling the MAC address authentication and port security function on one port at the same time.
- We cannot enable the MAC address authentication function and secure channel authentication function on one port at the same time.

Configure MAC Address Authentication User Name Format

The user name and password format used by the MAC address authentication includes two cases: fixed user name and password format and MAC address user name and password format.

Fixed user name and password format: When receiving the packets of the end user, the authentication device sends the configured user name and password to the authentication server for authentication.

MAC address user name and password format: The authentication device takes the MAC address of the end user as the user name and password. The MAC address format as the user name and password includes two cases: One is with the hyphen, such as 94-ae-e3-00-00-01; the other is not with hyphen, such as 94aee3000001.

Table 61–15 Configure MAC Address Authentication User Name Format

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure the MAC address authentication user name format	**dot1x mac-authentication user-name-format** { **fixed account** *account-value* **password** *password-value* | **mac-address** [**with-hyphen** | **without-hyphen**] }	Mandatory By default, the MAC address authentication adopts the MAC address with hyphen as the user name and password.

61.2.5 Configure Public Attributes *-B -S -E -A*

When configuring the public attribute parameters and if the 802.1X authentication function, secure channel authentication, or MAC address authentication function is not enabled in the port, the configured function does not take effect.

Configuration Conditions

None

Configure Authentication Failure Record Log Function

After enabling the authentication failure record log function, the authentication device will record the information about the authentication failure, so as to detect the fault reason.

Table 61-16 Configure Authentication Failure Record Log Function

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface. After entering the aggregation group configuration mode, the subsequent
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		configuration just takes effect on the aggregation group.
Configure the log function of recording the authentication failure	**dot1x syslog** { **enable** | **disable** }	Mandatory By default, the authentication failure record log function in the port is disabled.

Configure Maximum Users of a Port

After the number of the authenticated users in the port reaches the configured threshold, the authentication system does not answer the new authentication request initiated by the user.

Table 61–17 Configure Maximum Users of a Port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the maximum users of the port	**dot1x port-control max-user-num** *max-uer-num-value*	Mandatory By default, the maximum number of the users permitted to be connected in the port is 256.

NOTE

- The port needs to be configured as the user-based access control mode (Macbased). Otherwise, the configured access users cannot take effect.

Configure IP ACL Prefix Name

After the end user authentication is successful, when the server sends the IP ACL with the number greater than 2000, it is required to configure the IP ACL with the name as "IP ACL prefix name+ACL number" on the device. For example, the server sends the ACL with the number as 2001 and then configure the IP ACL with the name as "assignacl-2001" on the device.

Table 61-18 Configure IP ACL Prefix Name

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the IP ACL prefix name	**dot1x number-acl-prefix** *number-acl-prefix-name*	Mandatory By default, the IP ACL prefix name is "assignacl-".

Configure Default Valid VLAN

When the interface control mode is the user-based access control mode and the server does not send the VLAN (Auto VLAN), this configuration can be used to specify the VLAN if the authenticated users are expected to communicated in the specified VLAN.

This function needs to meet the following requirements to ensure normal running.

- The interface access control mode is the user-based access control mode (Macbased).
- The interface VLAN mode is the Hybrid mode.
- The MAC VLAN function is enbaled on the interface.

Table 61-19 Configure Default Valid VLAN

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the default valid VLAN	**dot1x default-active-vlan** *default-active-vlan-id*	Mandatory By default, the default valid VLAN is not configured.

NOTE

- When the user-based access control mode (Macbased) is configured on the interface,the priority of the binding relationship after the user authentication is in the following order: server sending the VLAN, default valid VLAN, VLAN which the PVID of the interface locates in.

Configure to Allow Unauthenticated User to Communicate in VLAN which PVID Locates in

When multiple interfaces access to the interface, each terminal needs to perform the access control. Some terminals that cannot initiate the 802.1X authentication also hopes to visit the network resources and you can enable the command. After the function is enabled, the unauthenticated end user can normally communicate in the VLAN which the PVID locates in.

This function must meet the following functions to ensure normal running.

- Enable the 802.1X authentication or MAC address authentication on the interface.
- The access control mode of the interface is the user-based access control mode (Macbased).
- The VLAN mode of the interface is the Hybrid mode.
- The function of only receiving the Untag packet needs to be enabled on the interface.

Table 61-20 Configure to Allow Unauthenticated User to Communicate in VLAN which PVID Locates in

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure to allow the unauthenticated user to communicate in the VLAN which the PVID locates in	**dot1x native-vlan-free**	Mandatory By default, the function of allowing the unauthenticated user to communicate in the VLAN which the PVID locates in is disabled,

NOTE

- After the function is enabled on the interface, the function of only receicing the untage packet needs to be enabled on the interface by configuring the **switchport accept frame-type untag** command on the interface to ensure that the packet sent by the unauthenticated user can only be forwarded in the VLAN which the PVID locates in.
- It is recommended that this function be used together with the VLAN sent by the server or the default valid VLAN.

Configure Port Access Control Mode

There are two kinds of port access control modes: port-based access control mode and user-based access control authentication mode.

Port-based access control mode (Portbased): In the port, only permit one user authentication to pass;

User-based access control mode (Macbased): In the port, permit multi-user authentication to pass. The users in the port need to pass the authentication respectively so that they can access the network.

Port-based access control mode includes two kinds: multi-host mode and single-host mode.

Multi-host mode (Multi-hosts): After one user in the port passes the authentication, the other users in the port can access the network without authentication.

Single-host mode (Single-host): In the port, only permit one user to pass the authentication and access the network; the other users cannot access the network and also cannot pass the authentication.

Table 61-21 Configure Port Access Control Mode

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the access control mode	**dot1x port-method** { **macbased** | **portbased** }	Mandatory By default, enable the user authentication mode in the port.
Configure the port-based access control mode	**dot1x port-method portbased host-mode** { **multi-hosts** | **single-host** }	Optional By default, enable the multi-host authentication mode in the port.

NOTE

- When configuring the host mode of the port-based access control mode, we need to ensure that the access control mode is configured as the port-based access control mode (Portbased).

Configure Guest VLAN

The user can get the 802.1X client software in Guest VLAN to upgrade the client, or execute other application program (such as anti-virus software and operation system patch) upgrade.

Table 61-22 Configure Guest VLAN

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure Guest VLAN	**dot1x guest-vlan** *guest-vlan-id*	Mandatory By default, Guest VLAN is not configured in the port; the value range is 1-4094.

NOTE

- Guest VLAN of the port cannot be applied to the dynamic VLAN. If VLAN ID specified by Guest VLAN is the VLAN automatically created by GVRP, Guest VLAN can be configured successfully, but cannot take effect.
- To ensure that the functions can be used normally, please distribute different VLAN IDs for Voice VLAN, Private VLAN, and Guest VLAN.

Configure Guest ACL

If the user is not authenticated or does not pass the authentication, we can configure Guest ACL in the port to limit the resources accessed by the user in Guest VLAN.

Table 61-23 Configure Guest ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure Guest ACL	**dot1x guest-acl** *guest-acl-name*	Mandatory By default, Guest ACL is not configured in the port.

NOTE

- If Guest VLAN is not configured in the port, the configured Guest ACL does not take effect.
- The ACL rule is configured in the authentication device.

Configure Timer Parameters

The timer parameters in the port contain: re-authentication timer, quiet timer, server timeout timer, client timeout timer, MAC address authentication user offline check timer.

Re-authentication timer (re-authperiod): After configuring the re-authentication function in the port, the authentication device regularly initiates the re-authentication request to the client, applicable to the 802.1X authentication.

Quiet timer (quiet-period): When the client reaches the maximum authentication failure times, the authentication device can answer the client authentication request again after the quiet time times out, applicable to the 802.1X authentication and MAC address authentication.

Server timeout timer (server-timeout): If the authentication device does not receive the response packet of the server within the specified time, it is regarded to be disconnected with the server, applicable to the 802.1X authentication and MAC address authentication.

Client timeout timer (supp-timeout): If the authentication device does not receive the response packet of the 802.1X client within the specified time, it is regarded to be disconnected with the user, applicable to the 802.1X authentication.

MAC address authentication user offline check timer (offline-detect): After enabling the MAC address authentication, the port periodically detects whether the user is online, applicable to the MAC address authentication.

Table 61-24 Configure Timer Parameters

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the timer parameters	**dot1x timeout** { **re-authperiod** *re-authperiod-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **offline-detect** *offline-detect-value* }	Mandatory By default, the re-authentication time in the port is 3600s; the value range is 5-65535; The quiet time is 60s; the value range is 1-65535; The timeout of the server is 30s; the value range is 5-3600; The timeout of the client is 30s; the value range is 5-3600; The offline check time of the client is 30s; the value range is 5-3600;

Restore Port Default Configuration

Restore the default configuration of the 802.1X authentication and MAC address authentication in the port.

Table 61–25 Restore Port Default Configuration

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Restore the default configuration of the port	**dot1x default**	Mandatory In the port, disable the 802.1X authentication and MAC address authentication function; the related configuration parameters are restored to the default values and the default configuration parameters do not take effect.

NOTE

- The command show dot1x is used to view the detailed authentication default configuration parameters.

Configure Log Record Step

When the user authentication failure time reaches the step value, the device records the authentication failure information to the logs.

Table 61-26 Configure Log Record Step

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the log record step	**dot1x auth-fail-count history** *auth-fail-history-step*	Mandatory By default, the log record step is 3.

61.2.6 802.1X Monitoring and Maintaining *-B -S -E -A*

Table 61-27 802.1X Monitoring and Maintaining

Command	Description
clear dot1x statistic [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **mac** { *mac-address* | **all** }]	Clear the authentication statistics information
clear dot1x auth-fail-user history [**mac** *mac-address*]	Clear the authentication failure record information
show dot1x	Display the default configuration information of the authentication
show dot1x auth-fail-user history [**recent** | **mac** *mac-address*]	Display the authentication failure information
show dot1x config { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* }	Display the configuration information of the authentication
show dot1x statistic [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **mac {** *mac-address* | **all** }]	Display the authentication statistics information
show dot1x free-ip	Display secure channel configuration information
show dot1x global config	Display the global configuration information

Command	Description
show dot1x user [**interface** *interface-name* | **link-aggregation** *link-aggregation-id* | **summary**]	Display the user information

61.3 802.1X Typical Configuration Example

61.3.1 Configure 802.1X Portbased Authentication *-B -S -E -A*

Network Requirements

1. The user PC1 and PC2 on one VLAN are connected to IP Network via Device. On Device, enable the 802.1X access control;
2. The authentication mode adopts the RADIUS authentication;
3. When the user does not pass the authentication, only permit accessing Update Server; after the user passes the authentication, permit accessing IP Network;
4. After one user on LAN passes authentication, the other users on the VLAN can access IP Network without authentication.

Network Topology

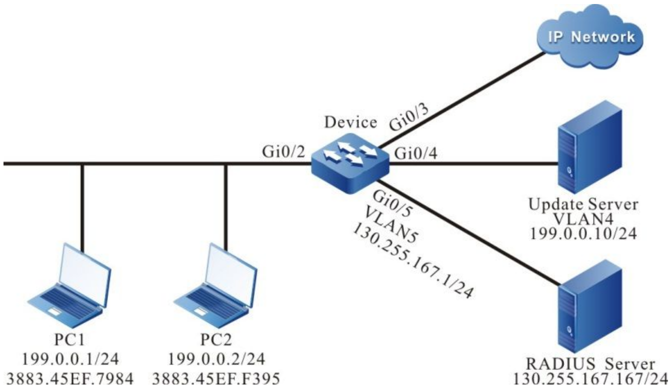


Figure 61–4 Networking of Configuring 802.1X Portbased Authentication

Configuration Steps

Step 1: Configure the link type of the VLAN and interface on Device.

#Create VLAN2–Vlan5 on Device.

```
Device#configure terminal
Device(config)#vlan 2-5
Device(config)#exit
```

#Configure the link type of interface gigabitethernet0/2 as Access, permitting the services of VLAN2 to pass

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the port link type on gigabitethernet0/3~gigabitethernet0/5 of Device as Access, permitting the services of VLAN3-VLAN5 to pass respectively. (Omitted)

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#exit
```

Step 3: Configure the AAA authentication.

#Enable the AAA authentication on Device, and adopt the RADIUS authentication mode. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24.

```
Device(config)#aaa new-model
Device(config)#aaa authentication connection default radius
Device(config)#radius-server host 130.255.167.167 priority 1 key admin
Device(config)#exit
```

Step 4: Configure the AAA server.

#Configure the user name, password and key as admin on the AAA server. (Omitted)

#On the AAA server, configure RADIUS to deliver the three attributes of Auto VLAN: 64 is VLAN, 65 is 802, and 81 is VLAN3. (Omitted)

Step 5: Configure the port 802.1X authentication.

#Enable the 802.1X authentication on the port and the authentication mode is Portbased.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#dot1x port-method portbased
Device(config-if-gigabitethernet0/2)#exit
```

#Configure Guest VLAN of the port as VLAN4.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x guest-vlan 4
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#Before passing the authentication, gigabitethernet0/2 is added to Guest VLAN. Here, PC1 and PC2 users are in VLAN4 and permit accessing Update Server.

```
Device#show vlan 4
---- ---- ------------------------------- ------- --------- ----------------------------
NO.  VID  VLAN-Name                       Owner   Mode      Interface
---- ---- ------------------------------- ------- --------- ----------------------------
```

```
1    4    VLAN0004                    static  Untagged  gi0/2  gi0/4
```

#Verify that PC1 can pass the authentication; the authentication server delivers VLAN3. Here, PC1 and PC2 users are in VLAN3 and can access IP Network.

```
Device#show dot1x user
--------------------
NO 1   : MAC_ADDRESS= 3883.45ef.7984  STATUS=     Authorized     USER_NAME=   admin
        VLAN=       3             IP_ADDRESS=  Unknown       INTERFACE=   gi0/2
        AUTH_STATE=  AUTHENTICATED   BACK_STATE=  IDLE          USER_TYPE=   DOT1X
        Online time: 0 week 0 day 0 hours 0 minute 51 seconds

 Total: 1    Authorized: 1   Unauthorized/guest: 0/0   Unknown: 0
```

61.3.2 Configure 802.1X Macbased Authentication *-B -S -E -A*

Network Requirements

1. The user PC1 and PC2 on one VLAN are connected to IP Network via Device. Device adopts the 802.1X access control;
2. The authentication mode adopts the RADIUS authentication;
3. When PC does not pass the authentication, only permit accessing Update Server; after passing the authentication, permit accessing IP Network;
4. After one user on LAN passes authentication, the other users on the VLAN still cannot access IP Network without passing the authentication.

Network Topology

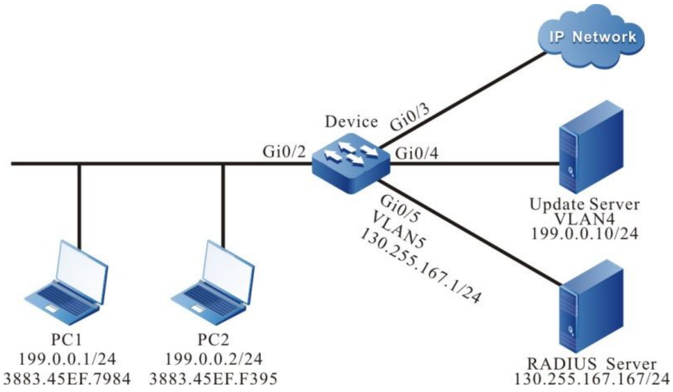


Figure 61-5 Networking of Configuring 802.1X Macbased Authentication

Configuration Steps

Step 1: Configure the link type of the VLAN and interface on Device.

#Create VLAN2–VLAN5 on Device.

```
Device#configure terminal
Device(config)#vlan 2-5
Device(config)#exit
```

#Configure the link type of interface gigabitethernet 0/2 as Hybrid, permitting services of VLAN2 to pass. Conifgure PVID as 2.

```
 Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the port link type on gigabitethernet0/3-gigabitethernet0/5 of Device as Access, permitting the services of VLAN3-VLAN5 to pass respectively. (Omitted)

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#exit
```

Step 3: Configure the AAA authentication.

#Enable the AAA authentication on Device, adopt the RADIUS authentication mode, the server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24.

```
Device(config)#aaa new-model
Device(config)#aaa authentication connection default radius
Device(config)#radius-server host 130.255.167.167 priority 1 key admin
```

Step 4: Configure the AAA server.

#Configure the user name, password and key as admin on the AAA server. (Omitted)

#On the AAA server, configure RADIUS to deliver the three attributes of Auto VLAN: 64 is VLAN, 65 is 802, and 81 is VLAN3. (Omitted)

Step 5: Configure the 802.1X authentication.

#Enable the 802.1X authentication on the port and configure the authentication mode as Macbased.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#dot1x port-method macbased
Device(config-if-gigabitethernet0/2)#exit
```

#Enable MAC VLAN of gigabitethernet0/2.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)exit
```

#Configure Guest VLAN of the port as VLAN4.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x guest-vlan 4
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#Before passing the authentication, gigabitethernet0/2 is added to Guest VLAN. Here, PC1 and PC2 users are in VLAN4, and PC1 and PC2 can access Update Server.

```
Device#show vlan 4
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Interface
---- ---- -------------------------------- ------- --------- -----------------------------
1    4    VLAN0004                         static  Untagged  gi0/2  gi0/4
```

#After the PC1 user initiates the authentication and passes the authentication, PC1 user is in Auto VLAN3 and can access IP Network. Here, PC2 still cannot access IP Network without authentication.

```
Device#show dot1x user
--------------------
NO 1   : MAC_ADDRESS= 3883.45ef.7984  STATUS=     Authorized      USER_NAME=   admin
         VLAN=       3              IP_ADDRESS=  Unknown       INTERFACE=   gi0/2
         AUTH_STATE=  AUTHENTICATED   BACK_STATE=  IDLE           USER_TYPE=   DOT1X
         Online time: 0 week 0 day 0 hours 0 minute 51 seconds

 Total: 1    Authorized: 1   Unauthorized/guest: 0/0   Unknown: 0
```

#After PC2 user inputs the wrong user name or password and failed to be authenticated, PC2 user is in Guest VLAN4 and can access Update Server.

```
Device#show dot1x user
--------------------
NO 1   : MAC_ADDRESS= 3883.45ef.7984  STATUS=     Unauth(guest)   USER_NAME=   admin
         VLAN=       4              IP_ADDRESS=  Unknown       INTERFACE=   gi0/2
         AUTH_STATE=  HELD          BACK_STATE=  IDLE           USER_TYPE=   DOT1X

Total:1     Authorized: 0   Unauthorized/guest: 0/1   Unknown: 0
```

61.3.3 Configure 802.1X Transparent Transmission Mode *-B -S -E -A*

Network Requirements

1. PC is connected to Device2 enabled with the 802.1X access control via Device1 and connected to IP Network.
2. Device1 enables the transparent transmission function; Device2 uses the RADIUS authentication mode.
3. After passing authentication, PC can access IP Network.

Network Topology

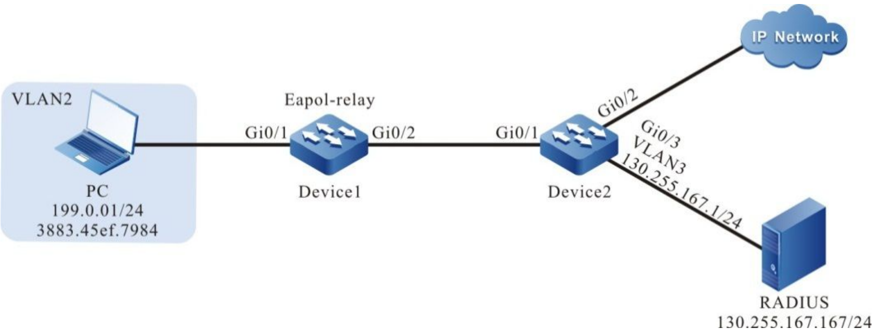


Figure 61-6 Networking of Configuring the 802.1X Transparent Transmission Mode

Configuration Steps

Step 1: Configure the link type of VLAN and interface on Device2.

#Create VLAN2–VLAN3 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2-3
Device2(config)#exit
```

#Configure the link type of interface gigabitethernet 0/1 as Access, permitting services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
```

#Configure the port link type on gigabitethernet0/2–gigabitethernet0/3 of Device2 as Access, permitting the services of VLAN2–VLAN3 to pass. (Omitted)

Step 2: Configure the interface IP address of Device2.

#Configure the IP address of VLAN3 as 130.255.167.1/24.

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
Device2(config-if-vlan3)#exit
```

Step 3: Configure the AAA authentication.

#Enable the AAA authentication on Device2, and adopt the RADIUS authentication mode. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24.

```
Device2(config)#aaa new-model
Device2(config)#aaa authentication connection default radius
Device2(config)#radius-server host 130.255.167.167 priority 1 key admin
Device2(config)#exit
```

Step 4: Configure the AAA server.

#Configure the user name, password, and key as admin on the AAA server. (Omitted)

Step 5: Configure the port VLAN of Device1.

#Configure the port link type on gigabitethernet0/1-gigabitethernet0/2 of Device1 as Access, permitting the services of VLAN2 to pass. (Omitted)

Step 6: Enable the 802.1X transparent transmission function on Device1.

#Configure the 802.1X transparent transmission mode on gigabitethernet0/1 of Device1 and the uplink port is gigabitethernet0/2.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#dot1x eapol-relay enable
Device1(config-if-gigabitethernet0/1)#dot1x eapol-relay uplink interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)#exit
```

Step 7: Configure the 802.1X authentication mode on Device2.

#Enable the 802.1X authentication of gigabitethernet0/1 and the port authentication mode is Portbased.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x port-control enable
Device2(config-if-gigabitethernet0/1)#dot1x port-method portbased
Device2(config-if-gigabitethernet0/1)#exit
```

Step 8: Check the result.

#PC user can be authenticated successfully and can access IP Network.

```
Device2#show dot1x user
--------------------
NO 1   : MAC_ADDRESS= 3883.45ef.7984  STATUS=     Authorized      USER_NAME=   admin
         VLAN=        3              IP_ADDRESS=  Unknown        INTERFACE=   gi0/2
         AUTH_STATE=  AUTHENTICATED   BACK_STATE=  IDLE           USER_TYPE=   DOT1X
         Online time: 0 week 0 day 0 hours 0 minute 51 seconds

 Total: 1    Authorized: 1   Unauthorized/guest: 0/0   Unknown: 0
```

61.3.4 Configure 802.1X Free-Client Authentication *-B -S -E -A*

Network Requirements

1. The network printer is connected to IP Network via Device; Device adopts the 802.1X access control;
2. Device regularly performs the offline detection for the network printer.
3. Use the RADIUS authentication mode.
4. After passing the authentication, the network printer can execute the printing task from IP Network.

Network Topology

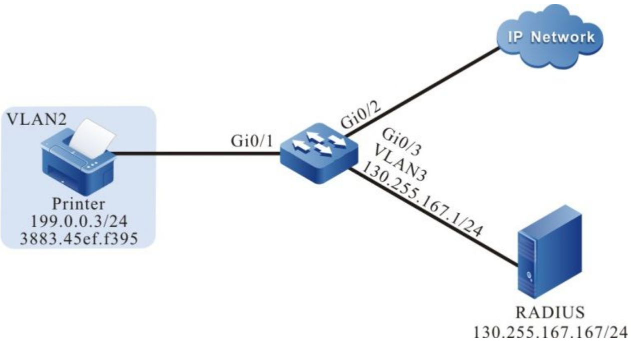


Figure 61-7 Networking of Configuring the 802.1X Free-Client Authentication

Configuration Steps

Step 1: Configure the link type of the VLAN and interface on Device.

#Create VLAN2–VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
Device(config)#exit
```

#Configure the link type of interface gigabitethernet 0/1 as Access, permitting services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#Configure the port link type on gigabitethernet0/2–gigabitethernet0/3 of Device as Access, permitting the services of VLAN2–VLAN3 to pass. (Omitted)

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN3 as 130.255.167.1/24.

```
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan3)#exit
```

Step 3: Configure the AAA authentication.

#Enable the AAA authentication on Device2, and adopt the RADIUS authentication mode. The server key is admin, the priority is 1, and the RADIUS server address is 130.255.167.167/24.

```
Device(config)#aaa new-model
Device(config)#aaa authentication connection default radius
Device(config)#radius-server host 130.255.167.167 priority 1 key admin
```

Step 4: Configure the AAA server.

#Configure the user name, password, and key as admin on the AAA server. (Omitted)

Step 5: Configure the 802.1X authentication.

#Configure the 802.1X free-client authentication mode, and use the MAC address of the network printer as user name and password.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dot1x mac-authentication enable
Device(config-if-gigabitethernet0/1)#exit
```

#Configure Device to perform the offline detection for the printer every 120s.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dot1x timeout offline-detect 120
Device(config-if-gigabitethernet0/1)#exit
```

Step 6: Check the result.

#The network printer can pass the authentication and can execute the printing task from IP Network.

```
Device#show dot1x user
--------------------
NO 1   : MAC_ADDRESS= 3883.45ef.f395  STATUS=     Authorized     USER_NAME=   38-83-45-ef-f3-95
         VLAN=        2              IP_ADDRESS=  199.0.0.3      INTERFACE=   gi0/2
         AUTH_STATE=  AUTHENTICATED   BACK_STATE=  IDLE          USER_TYPE=   MAC
         Online time: 0 week 0 day 0  hours 1  minutes 6 seconds

Total: 1     Authorized: 1   Unauthorized/guest: 0/0   Unknown: 0
```

61.3.5 Configure Secure Channel *-B -S -E -A*

Network Requirements

- User PC1 and PC2 on the same VLAN access the IP network through Device. Enable the secure channel access control on Device.
- Authentication adopts the RADIUS authentication.
- PC1 is allowed to visit Update Server before authentication success and is allowed to visit Update Server and IP Network after authentication success.
- PC2 is allowed to visit Update Server and IP Network without authentication.

Network Topology

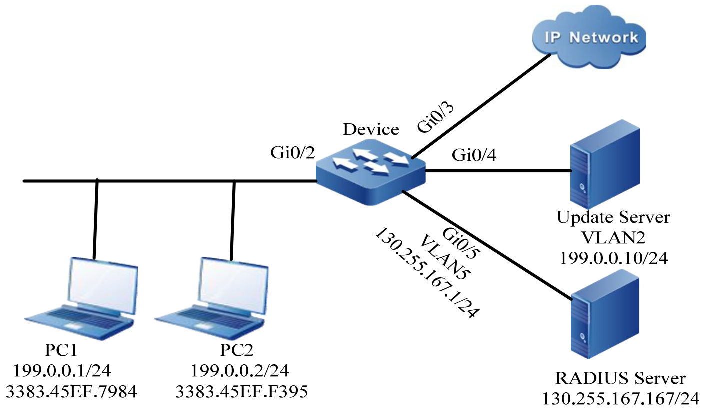


Figure 8–8 Networking of Configuring Secure Channel

Configuration Steps

Step 1: Configure the link type of the VLAN and interface on the interface.

#Create VLAN2 and VLAN5 on Device.

```
Device#configure terminal
Device(config)#vlan 2,5
Device(config)#exit
```

#Configure the link type of interface gigabitethernet0/2 as Access, permitting services of VLAN2 to pass.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)# switchport mode access
Device(config-if-gigabitethernet0/2)# switchport access vlan 2
Device(config-if-gigabitethernet0/2)#end
```

#Configure link type of interface gigabitethernet 0/3–gigabitethernet 0/4 as Access on Device, permitting services of VLAN2 to pass. Configure the link type of interface gigabitethernet 0/5 as Access, permitting services of VLAN5 to pass. (Omitted)

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN5 as 130.255.167.1/24.

```
Device#configure terminal
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#end
```

Step 3: Configure AAA authentication.

#Enable AAA authentication on Device and adopt the RADIUS authentication mode. Configure the server key as admin, priority as 1, and IP address of RADIUS server as 130.255.167.167/24.

```
Device#configure terminal
Device(config)#aaa new-model
Device(config)#aaa authentication connection default radius
Device(config)#radius-server host 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#Configure the user name, password, and key value on the AAA server as admin. (Omitted)

Step 5: Configure secure channel.

#Enable the secure channel access control on the interface gigabitethernet 0/2.

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x free-ip
Device(config-if-gigabitethernet0/2)#exit
```

#Configure a secure channel named channel and configure to allow PC1 to visit Update Server and conifgure to allow PC2 to visit Update Server and IP Network.

```
Device#configure                                                                                      terminal
Device(config)#hybrid access-list advanced channel
Device (config-adv-hybrid-nacl)#permit ip any any host 199.0.0.10 any
Device(config-adv-hybrid-nacl)#permit ip host 199.0.0.2 any any any
```

#Apply the secure channel named channel.

```
Device#configure terminal
Device(config)#global security access-group channel
Device(config)#exit
```

Step 6: Check the result.

#View the secure channel configuration information.

```
Device#show dot1x free-ip
802.1X free-ip Enable Interface (num:1): gi0/2

global security access-group channel

Total free-ip user number    : 0


Device#show hybrid access-list channel
hybrid access-list advanced channel
10    permit    ip    any    any    host    199.0.0.10    any
20 permit ip host 199.0.0.2 any any any
```

It can be viewed that the secure channel is enbaled on the interface gigabitethernet 0/2 and the interface is bound to the channel secure channel rule.

#PC1 can viist the Update Server and cannot visit other network resources before the authentication success.

#View the user authentication information after user PC1 initiates the authentication and authentication succeeds.

```
Device#show dot1x user
--------------------
NO 1   : MAC_ADDRESS= 3883.45ef.7984  STATUS=     Authorized     USER_NAME=   admin
         VLAN=       2          IP_ADDRESS=  199.0.0.1      INTERFACE=   gi0/2
         AUTH_STATE=  AUTHENTICATED   BACK_STATE=  IDLE          USER_TYPE=   DOT1X
         Online time: 0 week 0 day 0 hours 0 minute 51 seconds

 Total: 1    Authorized: 1   Unauthorized/guest: 0/0   Unknown: 0
```

It can be viewed that user PC1 has passed the authentication and then PC1 can visit Update Server and IP Network.

#PC2 can visit Update Server and IP Network without authentication.

61.3.6 Configure IP Authorization DHCP Server Mode *-B -S -E -A*

Network Requirements

- PC accesses IP Network via Device, Device 802.1X access control is enabled;
- Authentication method: RADIUS authentication is used;
- PC1 after acquiring IP address from designated DHCP Server can access the IP Network;
- PC2 will not be able to access the IP Network once it is configured carry static IP address authentication.

Network Topology

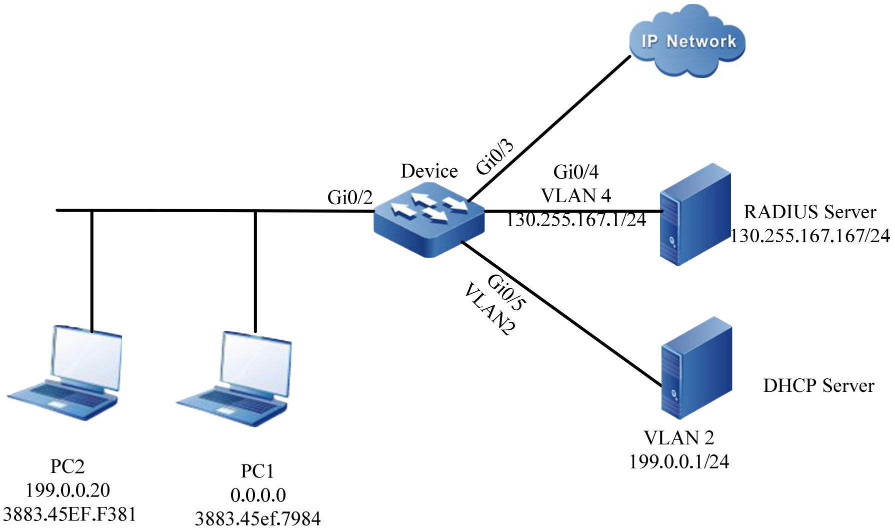


Figure 8-11 Networking Diagram - Configure 802.1X IP Authorization DHCP Server Mode

Configuration Steps

Step 1: On the Device, configure VLAN and the port link types.

#On the Device, create VLAN2, VLAN4; on gigabitethernet0/2 configure the port link type to Hybrid to allow the pass of VLAN2 business and configure PVID to 2.

```
Device#configure terminal
Device(config)#vlan 2,4
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#On device's gigabitethernet0/5, configure the port link type to Access to allow for the pass of VLAN2 business. (omitted)

#On device's gigabitethernet0/4, configure the port link type to Access to allow for the pass of VLAN4 business. (omitted)

Step 2: Configure Device's interface IP address.

#Configure VLAN4's IP address to 130.255.167.1/24.

```
Device(config)#intergice vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#On the Device, turn on AAA authentication in RADIUS mode, server cryptographic key: admin, priority level: 1, RADIUS server address: 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#Configure User Name and Password and Cryptographic Key Value to admin on AAA server. (omitted)

Step 5: Configure DHCP server.

#On DHCP server, configure the assigned IP address segment to 199.0.0.2-199.0.0.10 and subnet mask to 255.255.255.0. (omitted)

Step 6: On the Device, enable DHCP Snooping function, configure device's port gigabitethernet0/5 as trusted port.

```
Device(config)#dhcp-snooping
Device(config)#intergice gigabitethernet 0/5
Device(config-if-gigabitethernet0/5)#dhcp-snooping trust
Device(config-if-gigabitethernet0/5)#exit
```

Step 7: On the Device, configure 802.1X authentication.

#Turn on gigabitethernet0/2's 802.1X authentication.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

#Configure gigabitethernet0/2's IP authentication mode to DHCP Server.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x authorization ip-auth-mode dhcp-server
Device(config-if-gigabitethernet0/2)#exit
```

#Enable gigabitethernet0/2's ARP keepalive.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x client-probe enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 8: Check the result.

#If successfully authenticated, PC1 user obtain IP address from DHCP server to access IP Network.

```
Device#show dot1x user
--------------------
NO 1   : MAC_ADDRESS= 3883.45ef.7984  STATUS=     Authorized     USER_NAME=   admin
         VLAN=      2           INTERFACE=   gi0/2        USER_TYPE=   DOT1X
         AUTH_STATE=  AUTHENTICATED   BACK_STATE=  IDLE          IP_ADDRESS=  199.0.0.3
         IPV6_ADDRESS= Unknown

         Online time: 0 week 0 day 0 hours 0 minutes 36 seconds

Total: 1   Authorized: 1   Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

#If PC2 user is in GET-IP status after the authentication, he/she will not be able to get IP address.

```
NO 1   : MAC_ADDRESS= 3883.45ef.f381  STATUS=     Unauthorized     USER_NAME=   admin
         VLAN=       2              INTERFACE=   gi0/2           USER_TYPE=   DOT1X
         AUTH_STATE=  GET_IP         BACK_STATE=  IDLE            IP_ADDRESS=  Unknown
         IPV6_ADDRESS= Unknown

         Online time: 0 week 0 day 0 hour 0 minute 34 seconds

Total: 1   Authorized: 0   Unauthorized/guest/critical: 1/0/0 Unknown: 0
```

#Authentication passed, PC2 is unable to access IP Network.

61.3.7 Configure 802.1X Critical VLAN *-B -S -E -A*

Network Requirements

- PC accesses IP Network via Device, Device 802.1X access control is enabled;
- Authentication method: RADIUS authentication is used;
- If the PC fails authentication because of server unreachability, it will be permitted to access Update Server only.

Network Topology

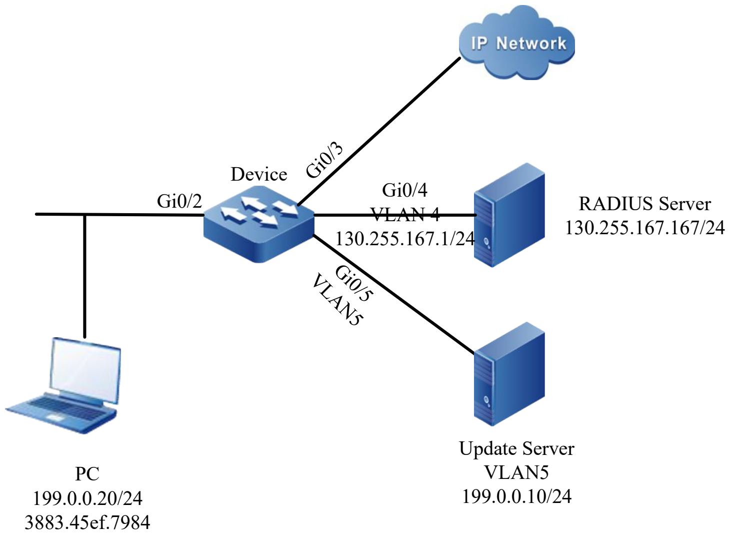


Figure 8-12 Networking Diagram - Configure 802.1X Critical VLAN

Configuration Steps

Step 1: On the Device, configure VLAN and the port link types.

#On the Device, create VLAN2, VLAN4, VLAN5; on gigabitethernet0/2 configure the port link type to Hybrid to allow the pass of VLAN2 business and configure PVID to 2.

```
Device#configure terminal
Device(config)#vlan 2,4,5
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#On device's gigabitethernet0/5, configure the port link type to Access to allow for the pass of VLAN5 business. (omitted)

#On device's gigabitethernet0/4, configure the port link type to Access to allow for the pass of VLAN4 business. (omitted)

Step 2: Configure Device's interface IP address.

#Configure VLAN4's IP address to 130.255.167.1/24.

```
Device(config)#intergice vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#On the Device, turn on AAA authentication in RADIUS mode, server cryptographic key: admin, priority level: 1, RADIUS server address: 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#Configure User Name and Password and Cryptographic Key Value to admin on AAA server. (omitted)

Step 5: On the Device, configure 802.1X authentication.

#Turn on gigabitethernet 0/2's 802.1X authentication.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

#Enable gigabitethernet0/2's MAC VLAN.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)exit
```

#Configure interface's Critical VLAN to VLAN5.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#authentication critical-vlan 5
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Check the result.

#If the user fails authentication because of server unreachability as a result of server malfunction that makes the Device unable to ping the server, the PC user will be permitted access to Update Server in the Critical VLAN.

Device#show dot1x user

```
--------------------
NO 1   : MAC_ADDRESS= 3883.45ef.7984  STATUS=     Unauth(critical)  USER_NAME=   admin
        VLAN=       5             INTERFACE=   gi0/2           USER_TYPE=   DOT1X
        AUTH_STATE=  CRITICAL_HELD   BACK_STATE=  IDLE            IP_ADDRESS=  Unknown
        IPV6_ADDRESS= Unknown


 Total: 1   Authorized: 0   Unauthorized/guest/critical: 0/0/1 Unknown: 0
```

#By that time, port gigabitethernet0/2 is added to Critical VLAN.

```
Device#show vlan 5
---- ---- -------------------------------- ------- --------- -----------------------------
NO.  VID  VLAN-Name                        Owner   Mode      Intergice
---- ---- -------------------------------- ------- --------- -----------------------------
1    5 VLAN5                        static  Untagged  gi0/2  gi0/5
```

61.3.8 Configure 802.1X and Secure Port Share *-B -S -E -A*

Network Requirements

- PC accesses IP Network via Device, Device 802.1X access control and port security are enabled;
- Authentication method: RADIUS authentication is used;
- Configure port security rules for PC1, which has no matching MAC address, so that PC1 can pass authentication to access IP network.
- Configure port security deny rules for PC2, which has matching MAC address, so that PC2 cannot pass authentication.

Network Topology

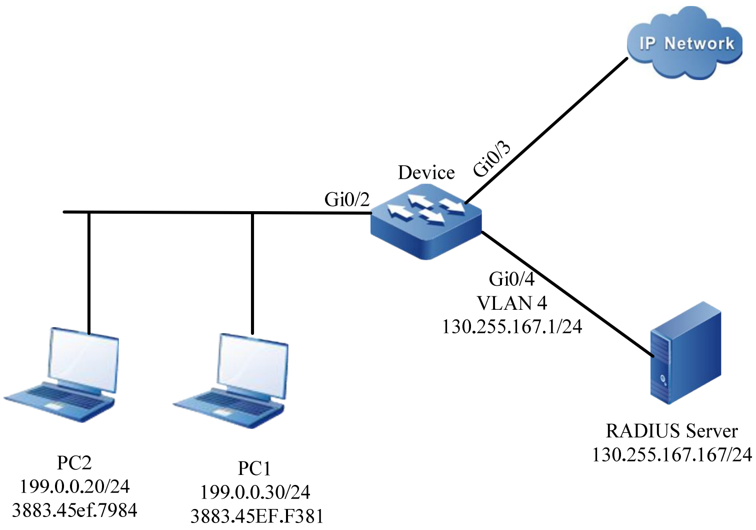


Figure 8-13 Networking Diagram - Configure 802.1X and Secure Port Share

Configuration Steps

Step 1: On the Device, configure VLAN and the port link types.

#On the Device, create VLAN2, VLAN4; on gigabitethernet0/2 configure the port link type to Hybrid to allow the pass of VLAN2 business and configure PVID to 2.

```
Device#configure terminal
Device(config)#vlan 2,4
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#On device's gigabitethernet0/4, configure the port link type to Access to allow for the pass of VLAN4 business. (omitted)

Step 2: Configure Device's interface IP address.

#Configure VLAN4's IP address to 130.255.167.1/24.

```
Device(config)#intergice vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure AAA authentication.

#On the Device, turn on AAA authentication in RADIUS mode, server cryptographic key: admin, priority level: 1, RADIUS server address: 130.255.167.167/24.

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

Step 4: Configure AAA server.

#Configure User Name and Password and Cryptographic Key Value to admin on AAA server. (omitted)

Step 5: On the Device, configure 802.1X authentication.

#Turn on gigabitethernet0/2's 802.1X authentication.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: On the Device, configure port security.

#On port gigabitethernet0/2, enable port security.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security enable
Device(config-if-gigabitethernet0/2)exit
```

#On port gigabitethernet0/2, configure port security rules.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security deny mac-address 3883.45EF.7984
Device(config-if-gigabitethernet0/2)exit
```

Step 7: Check the result.

#PC1 user can be successfully authenticated and can access IP Network after authentication.

```
Device#show dot1x user

--------------------

NO 1   : MAC_ADDRESS= 3883.45ef.f381  STATUS=      Authorized       USER_NAME=   admin
         VLAN=       2              INTERFACE=   gi0/2            USER_TYPE=   DOT1X
         AUTH_STATE=  AUTHENTICATED   BACK_STATE=  IDLE             IP_ADDRESS=  Unknown
         IPV6_ADDRESS= Unknown

         Online time: 0 week 0 day 0 hour 0 minute 1 second

 Total: 1   Authorized: 1   Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

#PC2 user authentication failed, unable to access the network.

62 ACL Configuration

62.1 Overview

62.1.1 Overview of ACL

One ACL (Access Control List) comprises a series of rules. Each rule is one permit, refuse or remark sentence, stating the corresponding matching condition and action. The ACL rule filters the packets by matching some field in the packet.

ACL can comprise multiple rules. The matching content specified by each rule is different and the matching contents in different rules may overlap or conflict. ACL rule matching strictly complies with the order of the sequence from small to large. The rule with smaller sequence takes effect earlier. Sequence means the order number of the rule in the while ACL.

There is one rule of refusing all packets hidden after the last rule of the ACL and the sequence is larger than all the other rules in the ACL. The hidden rule is invisible and it drops the packets that do not match the previous rules, that is, when the packet does not match with the previous rules, it matches the default rule and is dropped.

According to the ACL usage, we can divide ACL to five kinds, that is, IP standard ACL, IP extended ACL, MAC standard ACL, MAC extended ACL, and Hybrid extended ACL. ACL name can use the number and also can use the customized character string. When ACL name uses the number, the corresponding ACL type and number value range are as follows:

- IP standard ACL: 1-1000;
- IP extended ACL: 1001-2000;
- MAC standard ACL: 2001-3000;
- MAC extended ACL: 3001-4000;
- Hybrid extended ACL: 5001-6000.

When the ACL name adopts the customized character string, all ACLs share one name space, that is, if IP standard ACL uses one name, the other ACL types cannot use the name.

ACL also can execute the corresponding action group according to the matching. For details, refer to “QoS Configuration Manual”.

62.1.2 Overview of Time Domain

The time domain is the set of the time segments. One time domain can contain zero to multiple time segments. The time range of the time domain is the union of the time segments.

The time segment has the following two kinds:

- Periodical time segment: Periodical time segment means to select one day or several days from Monday to Sunday, and the start time point to the end time point as the time segment, taking effect every week repeatedly.
- Absolute time segment: The absolute time segment means to take effect within the specified date and time range

The user usually has the following demands:

The PC of one network segment can access the server only in the work time of the work day (except for all holidays); in the afternoon of Saturday, permit all PCs to communicate with the external Internet.

The communication control demands based on the time can be met by binding time domain in the ACL or ACL rule.

62.2 ACL Function Configuration

Table 62-1 ACL Function Configuration List

Configuration Task	
Configure the IP standard ACL	Configure the IP standard ACL
	Configure the IP standard ACL named by numbers
Configure the IP extended ACL	Configure the IP extended ACL
	Configure the IP extended ACL named by numbers
Configure the MAC standard ACL	Configure the MAC standard ACL
	Configure the MAC standard ACL named by numbers
Configure the MAC extended ACL	Configure the MAC extended ACL
	Configure the MAC extended ACL named by numbers
Configure the Hybrid extended ACL	Configure the Hybrid extended ACL
	Configure the Hybrid extended ACL named by numbers
Configure the quantity limitation of the ACL rules	Configure the quantity limitation of the ACL rules
Configure the time domain	Configure the time domain

Configuration Task	
	Configure the periodical time segment
	Configure the absolute time segment
	Configure the refresh period
	Configure the maximum time offset
	Configure the time domain to be bound with the ACL rule
	Configure the time domain to be bound with the ACL
Configure the ACL application	Configure IP ACL to be applied to the port
	Configure MAC ACL to be applied to the port
	Configure IP ACL to be applied to VLAN
	Configure IP ACL to be applied globally
	Configure Hybrid ACL to be applied globally
	Configure IP ACL to be applied to the interface
	Configure MAC ACL to be applied to the interface

62.2.1 Configure IP Standard ACL *-B -S -E -A*

IP standard ACL makes the rules according to the source IP address to filter the packets.

Configuration Conditions

None

Configure IP Standard ACL

IP standard ACL name can use the number and also can use the customized character string. If the IP standard ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired.

Table 62-2 Configure IP Standard ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP standard ACL	**ip access-list standard** { *access-list-number* | *access-list-name* }	Mandatory By default, the IP standard ACL is not configured. The number range of the IP standard ACL is 1-1000.
Configure the permit rule of ACL	[*sequence*] **permit** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Optional By default, the ACL permit rule is not configured.
Configure the refuse rule of ACL	[*sequence*] **deny** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of the ACL rule are not configured.

NOTE

- When using the **ip access-list standard** command to create the IP standard ACL, the ACL can be created only after configuring the rules in the IP standard ACL configuration mode.

- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure IP Standard ACL Named by Numbers

The IP standard ACL named by numbers can let the user identify the type of the ACL quickly. However, the IP standard ACL named by numbers has some limitations. For example, the ACL quantity is limited.

Table 62-3Configure IP Standard ACL Named by Numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP standard ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Mandatory By default, the IP standard ACL named by numbers is not configured. The sequence range of the IP standard ACL is 1-1000.
Configure the remarks of the IP standard ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the IP standard ACL named by numbers are not configured.

NOTE

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

62.2.2 Configure IP Extended ACL *-B -S -E -A*

IP extended ACL can make the classification rule according to the IP protocol number, source IP address, destination IP address, source TCP/UDP port number, destination TCP/UDP port number, packet priority, TCP tag, and fragment tag to filter the packets.

Configuration Conditions

None

Configure IP Extended ACL

IP extended ACL name can use the number and also can use the customized character string. If the IP extended ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired. IP extended ACL is richer, more correct, and more flexible than the contents defined by IP standard ACL.

Table 62-4 Configure IP Extended ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP extended ACL	**ip access-list extended** { *access-list-number* | *access-list-name* }	Mandatory By default, IP extended ACL is not configured. The sequence range of the IP extended ACL is 1001-2000.
Configure the permit rule of ACL	[*sequence*] **permit** *protocol* { **any** | *source-addr source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [**ack** | **fin** | **psh** | **rst** | **syn** | **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-**	Optional By default, the permit rule of ACL is not configured.

Step	Command	Description
	action-group *vfp-action-group-name*]	
Configure the refuse rule of ACL	[*sequence*] **deny** *protocol* { **any** | *source-addr source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [**ack** | **fin** | **psh** | **rst** | **syn** | **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of the ACL are not configured.

NOTE

- When using the **ip access-list extended** command to create the IP extended ACL, the ACL can be created only after configuring the rules in the IP extended ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure IP Extended ACL Named by Numbers

The IP extended ACL named by numbers can let the user identify the type of the ACL quickly. However, the IP extended ACL named by numbers has some limitations. For example, the ACL quantity is limited. IP extended ACL is richer, more correct, and more flexible than the contents defined by IP standard ACL.

Table 62-5Configure IP Extended ACL Named by Numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the IP extended ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } *protocol* { **any** | *source-addr source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [**ack** | **fin** | **psh** | **rst** | **syn** | **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Mandatory By default, the IP extended ACL named by numbers is not configured. The sequence range of the IP extended ACL is 1001-2000.
Configure the remarks of the IP extended ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the IP extended ACL named by numbers are not configured.

NOTE

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

62.2.3 Configure MAC Standard ACL *-B -S -E -A*

MAC standard ACL makes the rules according to the source MAC address to filter the packets.

Configuration Conditions

None

Configure MAC Standard ACL

MAC standard ACL name can use the number and also can use the customized character string. If the MAC standard ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired.

Table 62-6 Configure MAC Standard ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the MAC standard ACL	**mac access-list standard** { *access-list-number* | *access-list-name* }	Mandatory By default, the MAC standard ACL is not configured. The sequence range of the MAC standard ACL is 2001-3000.
Configure the permit rule of ACL	[*sequence*] **permit** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**l2-action-group** *l2-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Optional By default, the permit rule of ACL is not configured.
Configure the refuse rule of ACL	[*sequence*] **deny** { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**l2-action-group** *l2-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional

Step	Command	Description
		By default, the remarks of ACL are not configured.

NOTE

- When using the **mac access-list standard** command to create the MAC standard ACL, the ACL can be created only after configuring the rules in the MAC standard ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure MAC Standard ACL Named by Numbers

The MAC standard ACL named by numbers can let the user identify the type of the ACL quickly. However, the MAC standard ACL named by numbers has some limitations. For example, the ACL quantity is limited.

Table 62-7Configure MAC Standard ACL Named by Numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the MAC standard ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } { **any** | *source-addr source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**l2-action-group** *l2-action-name*] [**egr-action-group** *egr-action-name*] [**vfp-action-group** *vfp-range-name*]	Mandatory By default, the MAC standard ACL named by numbers is not configured. The sequence range of the MAC standard ACL is 2001-3000.
Configure the remarks of the MAC standard ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the MAC standard ACL named by numbers are not configured.

NOTE

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

62.2.4 Configure MAC Extended ACL *-B -S -E -A*

MAC extended ACL can make the classification rule according to the Ethernet protocol type, source MAC address, destination MAC address, VLAN ID, and 802.1p priority, so as to filter the packets.

Configuration Conditions

None

Configure MAC Extended ACL

MAC extended ACL name can use the number and also can use the customized character string. If the MAC extended ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired. MAC extended ACL is richer, more correct, and more flexible than the contents defined by MAC standard ACL.

Table 62-8 Configure MAC Extended ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the MAC extended ACL	**mac access-list extended** { *access-list-number* | *access-list-name* }	Mandatory By default, MAC extended ACL is not configured. The sequence range of the MAC extended ACL is 3001-4000.
Configure the permit rule of ACL	[*sequence*] **permit** { **any** | *source-addr source-wildcard* | **host** *source-addr* } { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [**ether-type** *type*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*] [**l2-action-group** *l2-action-group-name*]	Optional By default, the permit rule of ACL is not configured.

Step	Command	Description
	[**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	
Configure the refuse rule of ACL	[*sequence*] **deny** { **any** | *source-addr source-wildcard* | **host** *source-addr* } { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [**ether-type** *type*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*] [**l2-action-group** *l2-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional By default, the remarks of ACL are not configured.

NOTE

- When using the **mac access-list extended** command to create the MAC extended ACL, the ACL can be created only after configuring the rules in the MAC extended ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure MAC Extended ACL Named by Numbers

The MAC extended ACL named by numbers can let the user identify the type of the ACL quickly. However, the MAC extended ACL named by numbers has some limitations. For example, the ACL quantity is limited. MAC extended ACL is richer, more correct, and more flexible than the contents defined by MAC standard ACL.

Table 62-9 Configure MAC Extended ACL Named by Numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the MAC extended ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } { **any** | *source-addr source-wildcard* | **host** *source-addr* } { **any** | *destination-addr destination-wildcard* | **host** *destination-addr* } [**ether-type** *type*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*] [**l2-action-group** *l2-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**vfp-action-group** *vfp-action-group-name*]	Mandatory By default, the MAC extended ACL named by numbers is not configured. The sequence range of the MAC extended ACL is 3001-4000.
Configure the remarks of the MAC extended ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the MAC extended ACL named by numbers are not configured.

NOTE

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

62.2.5 Configure Hybrid Extended ACL *-B -S -E -A*

Hybrid extended ACL can make the classification rule according to the IP protocol type, source IP address, source MAC address, packet priority, VLAN ID, and 802.1p priority, so as to filter the packets.

Configuration Conditions

None

Configure Hybrid Extended ACL

Hybrid extended ACL name can use the number and also can use the customized character string. If the Hybrid extended ACL name adopts the numbers, we can configure the maximum quantity limitation of ACL; if adopting the customized character string, there is no limitation for the maximum quantity of ACL. The user can select the ACL name as desired. Hybrid extended ACL is richer, more correct, and more flexible than using the contents defined by IP ACL and MAC ACL separately, but Hybrid extended ACL can only be applied globally and can only filter the received packets.

Table 62-10 Configure Hybrid Extended ACL

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the Hybrid extended ACL	**hybrid access-list extended** { *access-list-number* | *access-list-name* }	Mandatory By default, Hybrid extended ACL is not configured. The sequence range of the Hybrid extended ACL is 5001-6000.
Configure the permit rule of ACL	[*sequence*] **permit** *protocol* { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *source-mac-addr source-wildcard* | **host** *source-mac-addr* } [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*]	Optional By default, the permit rule of ACL is not configured.
Configure the refuse rule of ACL	[*sequence*] **deny** *protocol* { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *source-mac-addr source-wildcard* | **host** *source-mac-addr* } [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*]	Optional By default, the refuse rule of ACL is not configured.
Configure the ACL remarks	[*sequence*] **remark** *comment*	Optional

Step	Command	Description
		By default, the remarks of ACL are not configured.

NOTE

- When using the **hybrid access-list extended** command to create the Hybrid extended ACL, the ACL can be created only after configuring the rules in the Hybrid extended ACL configuration mode.
- Sequence means the order number of the rule in the ACL. ACL matches and filters the packet strictly according to the order from small sequence to large sequence. The rule with the small sequence first takes effect. When all rules do not match, execute the default drop action, that is, all the packets not permitted to pass are dropped.

Configure Hybrid Extended ACL Named by Numbers

The Hybrid extended ACL named by numbers can let the user identify the type of the ACL quickly. However, the Hybrid extended ACL named by numbers has some limitations. For example, the ACL quantity is limited.

Table 62-11 Configure the Hybrid Extended ACL Named by Numbers

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the Hybrid extended ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } *protocol* { **any** | *source-ip-addr source-wildcard* | **host** *source-ip-addr* } { **any** | *source-mac-addr source-wildcard* | **host** *source-mac-addr* } [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**cos** *cos*] [**vlan-id** *vlan*] [**time-range** *time-range-name*]	Mandatory By default, the Hybrid extended ACL named by numbers is not configured. The sequence range of the Hybrid extended ACL is 5001-6000.
Configure the remarks of the Hybrid extended ACL named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, the remarks of the Hybrid extended ACL named by numbers are not configured.

NOTE

- If the ACL with the specified sequence does not exist, create one new ACL and add new rules. If the ACL with the specified number exists, just add new rules.

62.2.6 Configure IPv6 Standard ACL *-B -S -E -A*

IPv6 standard ACL can, depending on source IPv6 address field. stipulate classification rules for filtering messages.

Configuration Conditions

None

Configure IPv6 Standard ACL

IPv6 standard ACL's name can be numbers or user customized character strings. If IPv6 standard ACL is named by numbers, the maximum limit of ACL numbers can be configured; if named using user customized character strings, the maximum limit of ACL numbers can be configured as None. User may, depending on the actual situation, select a suitable ACL name.

Table 11-12 Configure IPv6 Standard ACL

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IPv6 standard ACL	**ipv6 access-list standard** { *access-list-number* | *access-list-name* }	Required By default, IPv6 standard ACL is not configured
Configure ACL permission rules	[*sequence*] **permit** { **any** | *source-addr/source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**pbr-action-group** *pbr-action-group-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*]	Optional By default, ACL permission rules are not configured

Steps	Command	Description
Configure ACL deny rules	[*sequence*] **deny** { **any** | *source-addr/source-wildcard* **|** **host** *source-addr* } [**time-range** *time-range-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**pbr-action-group** *pbr-action-group-name*]	Optional By default, ACL deny rules are not configured
Configure ACL annotation	[*sequence*] **remark** *comment*	Optional By default, ACL rules annotation is not configured

NOTE

- When creating IPv6 standard Access Control list with command **ipv6 access-list standard**, the Access Control list can be created only after rules have been configured in IPv6 standard Access Control list configuration mode.
- Sequence refers to the sequence number of the rule in the entire ACL. When performing matched filtering of messages with ACL, the filtering will be carried out in strict ascending order of sequence. Rules of smaller sequence apply first. When no rules match, the default action Discard will be carried out, i.e., all messages that have not passed will be rejected.

Configure IPv6 Standard ACL Named by Numbers

IPv6 standard ACL rules named by numbers help user to fast identify the type of rule access control list. However, IPv6 standard ACL named by numbers is subjected to certain limitations, such as: the number of access lists is limited, the user identification ACL rules is complicated, etc.

Table 62-13 Configure IPv6 Standard ACL Named by Numbers

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IPv6 standard ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** }	Required

Steps	Command	Description
	{ **any** | *source-addr/source-wildcard* | **host** *source-addr* } [**time-range** *time-range-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*] [**pbr-action-group** *pbr-action-group-name*]	By default, IPv6 standard ACL named by numbers is not configured IPv6 standard ACL can be numbered in the range of 6001~7000
Configure IPv6 standard ACL annotation named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, IPv6 standard ACL annotation named by numbers is not configured

NOTE

- If ACL of designated ID does not exist, then create a new ACL and add new rules. If ACL of designated ID does exist, then add new rules only.

62.2.7 Configure IPv6 Extended ACL *-B -S -E -A*

IPv6 extended ACL can, depending on such fields as IPv6 protocol number, source IPv6 address, destination IPv6 address, source TCP/UDP port ID, destination TCP/UDP port ID, message priority level, and TCP flag, stipulate classification rules for filtering the messages.

Configuration Conditions

None

Configure IPv6 Extended ACL

IPv6 extended ACL's name can be numbers or user customized character strings. If IPv6 extended ACL is named by numbers, the maximum limit of ACL numbers can be configured; if named using user customized character strings, the maximum limit of ACL numbers can be configured as None. User may, depending on the actual situation, select a suitable ACL name.

Table 62-14 Configure IPv6 Extended ACL

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IPv6 extended ACL	**ipv6 access-list extended** { *access-list-number* | *access-list-name* }	Required By default, IPv6 extended ACL is not configured
Configure ACL permission rules	[*sequence*] **permit** *protocol* { **any** | *source-addr/source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr*/*destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [**ack** / **fin** / **psh** / **rst** / **syn** / **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**pbr-action-group** *pbr-action-group-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*]	Optional By default, ACL permission rules are not configured
Configure ACL deny rules	[*sequence*] **deny** *protocol* { **any** | *source-addr/source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr*/*destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [**ack** / **fin** / **psh** / **rst** / **syn** / **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**pbr-action-group** *pbr-action-group-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*]	Optional By default, ACL deny rules are not configured
Configure ACL annotation	[*sequence*] **remark** *comment*	Optional

Steps	Command	Description
		By default, ACL rules annotation is not configured

NOTE

- When creating IPv6 extended Access Control list with command **ipv6 access-list extended**, the Access Control list can be created only after rules have been configured in IPv6 extended Access Control list configuration mode.
- Sequence refers to the sequence number of the rule in the entire ACL. When performing matched filtering of messages with ACL, the filtering will be carried out in strict ascending order of sequence. Rules of smaller sequence apply first. When no rules match, the default action Discard will be carried out, i.e., all messages that have not passed will be rejected.

Configure IPv6 Extended ACL Named by Numbers

IPv6 extended ACL rules named by numbers help user to fast identify the type of rule access control list. However, IPv6 extended ACL named by numbers is subjected to certain limitations, such as: the number of access lists is limited, the user identification ACL rules is complicated, etc.

Table 62-15 Configure IPv6 Extended ACL Named by Numbers

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IPv6 extended ACL named by numbers	**access-list** *access-list-number* { **permit** | **deny** } *protocol* { **any** | *source-addr/source-wildcard* | **host** *source-addr* } [*operator source-port*] { **any** | *destination-addr/destination-wildcard* | **host** *destination-addr* } [*operator destination-port*] [**ack** / **fin** / **psh** / **rst** / **syn** / **urg**] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*] [**pbr-action-group** *pbr-action-group-name*] [**l3-action-group** *l3-action-group-name*] [**egr-action-group** *egr-action-group-name*]	Required By default, IPv6 extended ACL named by numbers is not configured IPv6 standard ACL can be numbered in the range of 7001~8000

Steps	Command	Description
Configure IPv6 extended ACL annotation named by numbers	**access-list** *access-list-number* **remark** *comment*	Optional By default, IPv6 extended ACL annotation named by numbers is not configured

NOTE

- If ACL of designated ID does not exist, then create a new ACL and add new rules. If ACL of designated ID does exist, then add new rules only.

62.2.8 Configure ACL Rule Quantity Limitation *-B -S -E -A*

Configuration Conditions

Before configuring the time domain function, first complete the following task:

- Configure ACL

Configure ACL Rule Quantity Limitation

After enabling the ACL rule quantity limitation, the maximum number of the rules that can be configured in one ACL is 1024.

Table 62-16 Configure the ACL Rule Quantity Limitation

Step	**Command**	**Description**
Enter global configuration mode	**configure terminal**	-
Disable/enable the ACL rule quantity limitation	**access-list rule-limit** { **disable** | **enable** }	Mandatory By default, it is enabled, that is, the maximum number of the rules that can be configured in one ACL is 1024.

62.2.9 Configure Time Domain *-B -S -E -A*

The time domain is the set of the time segments. One time domain can contain zero to multiple time segments. The time range of the time domain is the union of the time segments. The time domain can be bound with ACL or ACL rule, as the condition of whether ACL or ACL rule takes effect.

Configuration Conditions

Before configuring the time domain function, first complete the following task:

- Configure ACL

Configure Time Domain

Configure whether the application object of the time domain is limited by the time domain. When it is enabled, the application object is limited by the time domain. On the contrary, it is not limited by the time domain.

Table 62-17 Configure Time Domain

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure disabling/enabling the time domain	**set time-range** { **enable | disable** }	Mandatory By default, it is enabled.

Configure Periodical Time Segment

Periodical time segment: Periodical time segment means to select one day or several days from Monday to Sunday, and the start time point to the end time point as the time segment, taking effect every week repeatedly.

Table 62-18 Configure Periodical Time Segment

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the time domain	**time-range** *time-range-name*	Mandatory By default, do not configure the time domain.
Configure the periodical time segment	[*sequence*] **periodic** [*days-of-the-week*]	Mandatory

Step	Command	Description
	[*hh:mm* [*:ss*]] **to** [*days-of-the-week*] [*hh:mm* [*:ss*]]	By default, do not configure periodical time segment.

Configure Absolute Time Segment

The absolute time segment means to take effect within the specified date and time range.

Table 62-19 Configure Absolute Time Segment

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the time domain	**time-range** *time-range-name*	Mandatory By default, do not configure the time domain.
Configure the absolute time segment of the time domain	[*sequence*] **absolute start** *hh:mm* [*:ss*] [*day* [*month* [*year*]]] **end** *hh:mm* [*:ss*] [*day* [*month* [*year*]]]	Mandatory By default, do not configure the absolute time segment of the time domain.

Configure Refresh Period

The status of time domain includes effective and ineffective. The status refresh period of the time domain is 1 minute by default. Automatically refresh according to the current system time. Therefore, when refreshing the status, there may be 0-60s delay compared with the system time.

Table 62-20 Configure Refresh Period

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the refresh period of the time domain	**set time-range frequency** *frequency-value*	Mandatory The default value is 1. The refresh period is the interval between two

Step	Command	Description
		refreshes and the unit is minute.

Configure Maximum Time Offset

The maximum offset means the maximum offset between accumulation time of the counter and the system time. Once the time statistics exceeds the offset, re-judge the status of the time domain and update during the next refreshing so that the time statistics is more correct.

Table 62-21 Configure Maximum Time Offset

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the maximum time offset of the time domain	**set time-range max-offset** *max-offset-value*	Mandatory The default value is 100. The unit of the time offset is second and the value range is 1-300.

Configure Time Domain and ACL Rule Binding

When it is necessary to control one user to access the network resources within the specified time segment, we can set the ACL rule based on the time domain to filter the packets. Whether the time domain takes effect directly affects the associated ACL rule.

Table 62-22 Configure Time Domain and ACL Rule Binding

Step	Command	Description
Configure the binding with IP standard ACL rule	Refer to “Configure IP Standard ACL”	-
Configure the binding with IP extended ACL rule	Refer to “Configure IP Extended ACL”	-
Configure the binding with MAC standard ACL rule	Refer to “Configure MAC Standard ACL”	-
Configure the binding with MAC extended ACL rule	Refer to “Configure MAC Extended ACL”	-

Step	Command	Description
Configure the binding with Hybrid extended ACL rule	Refer to “Configure Hybrid Extended ACL”	-

NOTE

- When the time domain bound with the ACL rule does not exist, the ACL rule is in the effective state.

Configure Time Domain and ACL Binding

When it is necessary to control one user to access the network resources within the specified time segment, we can set the ACL rule based on the time domain to filter the packets. Whether the time domain takes effect directly affects the rules contained in the whole ACL.

Table 62-23 Configure Time Domain and ACL Binding

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the time domain to be bound with IP ACL	**ip time-range** *time-range-name* **access-list** { *access-list-number* | *access-list-name* }	Mandatory By default, do not configure the time domain to be bound with IP ACL.
Configure the time domain to be bound with MAC ACL	**mac time-range** *time-range-name* **access-list** { *access-list-number* | *access-list-name* }	Mandatory By default, do not configure the time domain to be bound with MAC ACL.
Configure the time domain to be bound with Hybrid ACL	**hybrid time-range** *time-range-name* **access-list** { *access-list-number* | *access-list-name* }	Mandatory By default, do not configure the time domain to be bound with Hybrid ACL.

NOTE

- When the time domain bound with the ACL rule does not exist, the ACL rule is in the effective state.

62.2.10 Configure ACL Application *-B -S -E -A*

ACL can be applied globally, to VLAN, port and interface. IP ACL can be applied globally, VLAN, the ingress and egress of the port and interface; Hybrid ACL can only be applied globally; MAC ACL can be applied to the ingress and egress of the port and interface.

If ACL is applied globally, filter all the ingress packets of the device port; if ACL is applied to VLAN, filter all ingress packets of the port in VLAN and the egress forwarding packets; if ACL is applied to the port, filter all ingress packets of the port and the egress forwarding packets; if ACL is applied to the interface, filter the packets that need to be processed on CPU at the ingress of the interface and the packets generated by the local CPU at the egress of the interface.

ACL matching has the priority order. The priority from high to low is to be applied to the port, applied to the VLAN, and applied globally.

If the packet matches the ACL rule of applying to port, VLAN and globally at the same time, the packet whose high priority filter result is permit is forwarded to the next-priority ACL for filtering. The packet whose high priority filter result is deny is dropped directly and is not forwarded to the next-priority ACL for processing any more.

Configuration Conditions

Before configuring the ACL application function, first complete the following task:

- Configure ACL

Configure IP ACL to Be Applied to Port

Apply IP ACL to the port. The packet passing the port is analyzed and processed according to IP ACL.

Table 62-24 Configure IP ACL to Be Applied to the Port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
		just takes effect on the aggregation group.
Configure applying IP ACL to the port	**ip access-group** { *access-list-number* | *access-list-name* } { **in** | **out** | **vfp** }	Mandatory By default, IP ACL is not applied to the port.

NOTE

- If ACL applied to the port does not exist, all packets passing the port are permitted.

Configure MAC ACL to Be Applied to Port

Apply MAC ACL to the port. The packet passing the port is analyzed and processed according to MAC ACL.

Table 62-25 Configure MAC ACL to Be Applied to the Port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure MAC ACL to be applied to the port	**mac access-group** { *access-list-number* | *access-list-name* } { **in** | **out** | **vfp** }	Mandatory By default, MAC ACL is not applied to the port.

NOTE

- If ACL applied to the port does not exist, all packets passing the port are permitted.

Configure IP ACL to Be Applied to VLAN

Apply IP ACL to the VLAN. The packet passing the port is analyzed and processed according to IP ACL.

Table 62-26 Configure IP ACL to Be Applied to VLAN

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the VLAN configuration mode	**vlan** *vlan-id*	-
Configure IP ACL to be applied to VLAN	**ip access-group** { *access-list-number* | *access-list-name* } { **in** | **out** | **vfp** }	Mandatory By default, VLAN is not applied to IP ACL.

NOTE

- If ACL applied to the VLAN does not exist, all packets passing the VLAN are permitted.

Configure IP ACL to Be Applied Globally

Apply IP ACL globally. The packets passing all ports are analyzed and processed according to IP ACL.

Table 62-27 Configure IP ACL to Be Applied Globally

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure IP ACL to be applied globally	**global ip access-group** { *access-list-number* | *access-list-name* } **in**	Mandatory By default, IP ACL is not applied globally.

NOTE

- If the ACL applied globally does not exist and all ports are not configured with ACL, all packets passing the port are permitted.

Configure Hybrid ACL to Be Applied Globally

Apply Hybrid ACL globally. The packets passing all ports are analyzed and processed according to Hybrid ACL.

Table 62-28 Configure Hybrid ACL to Be Applied Globally

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure Hybrid ACL to be applied globally	**global hybrid access-group** { *access-list-number* | *access-list-name* } **in**	Mandatory By default, Hybrid ACL is not applied globally.

NOTE

- If the ACL applied globally does not exist and all ports are not configured with ACL, all packets passing all ports are permitted.
- When configuring Hybrid ACL to be applied globally, the global IP Source Guard function needs to be disabled.

Configure IP ACL to Be Applied to Interface

Apply IP ACL to the interface. The packet passing the port is analyzed and processed according to IP ACL.

Table 62-29 Configure IP ACL to Be Applied to the Interface

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-

Step	Command	Description
Configure IP ACL to be applied to the interface	**ip access-group** { *access-list-number* | *access-list-name* } { **in** | **out** | **self** }	Mandatory By default, IP ACL is not applied to the interface.

NOTE

- If ACL applied to the interface does not exist, all packets passing the interface are permitted.

Configure MAC ACL to Be Applied to Interface

Apply MAC ACL to the interface. The packet passing the port is analyzed and processed according to MAC ACL.

Table 62-30 Configure MAC ACL to Be Applied to the Interface

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure MAC ACL to be applied to the interface	**mac access-group** { *access-list-number* | *access-list-name* } { **in** | **out** }	Mandatory By default, MAC ACL is not applied to the interface.

NOTE

- If ACL applied to the interface does not exist, all packets passing the interface are permitted.

62.2.11 ACL Monitoring and Maintaining *-B -S -E -A*

Table 62-31 ACL Monitoring and Maintaining

Command	Description
show access-list [*access-list-number* | *access-list-name*]	Display the ACL configuration information
show acl-object [**global** | **interface** [**in** | **out** | **vfp**] | **vlan** [**in** | **out**]]	Configure the information of the ACL applied to VLAN, port and globally
show ip access-list [*access-list-number* | *access-list-name*]	Configure the IP ACL configuration information
show ip interface list	Display the information of the IP ACL applied to the interface
show ipv6 access-list [*access-list-number* | *access-list-name*]	Display the configuration information of the IPv6 ACL
show mac access-list [*access-list-number* | *access-list-name*]	Configure the MAC ACL configuration information
show mac interface list	Display the information of the MAC ACL applied to the interface
show time-range [*time-range-name*]	Display the configuration and status information of the time domain

62.3 ACL Typical Configuration Example

62.3.1 Configure IP Standard ACL

-B -S -E -A

Network Requirements

- PC1, PC2, and PC3 are connected to IP Network via Device.
- Configure the IP standard ACL rule, realizing that PC1 can access IP Network, PC2 and PC3 cannot access IP Network.

Network Topology

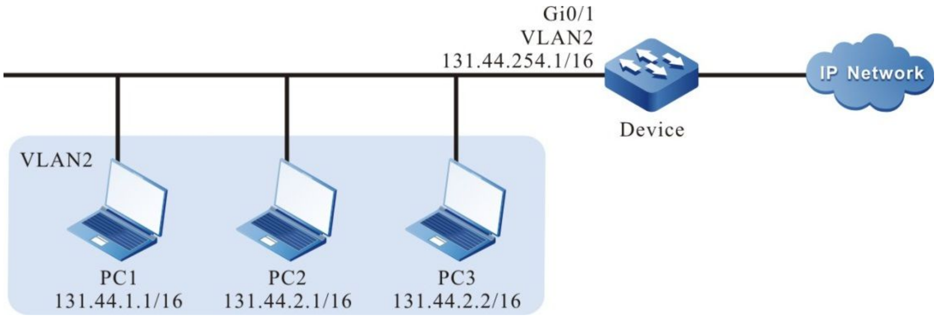


Figure 62–1 Networking of Configuring IP Standard ACL

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the corresponding VLAN interface and IP address on Device. (Omitted)

Step 3: Configure the IP standard ACL.

#Configure the IP standard ACL with serial number 1 on Device.

```
Device(config)#ip access-list standard 1
```

#Configure the rule, permitting PC1 to access IP Network.

```
Device(config-std-nacl)#permit host 131.44.1.1
```

#Configure the rule, preventing the network segment 131.44.2.0/24 from accessing IP Network.

```
Device(config-std-nacl)#deny 131.44.2.0 0.0.0.255
Device(config-std-nacl)#exit
```

#View the information of the ACL with serial number 1 on Device.

```
Device#show ip access-list 1
ip access-list standard 1
 10 permit host 131.44.1.1
 20 deny 131.44.2.0 0.0.0.255
```

Step 4: Configure applying IP standard ACL.

#Apply the IP standard ACL with serial number 1 to the ingress of port gigabitethernet0/1 on Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1                    IN           IP         1
```

Step 5: Check the result.

#PC1 can access IP Network; PC and PC3 cannot access IP Network.

62.3.2 Configure IP Extended ACL with Time Domain *-B -S -E -A*

Network Requirements

- PC1, PC2, and PC3 are connected to IP Network via Device.
- Configure the IP extended ACL rule, realizing that PC1 can access IP Network within the specified time, PC2 can access the FTP service in IP Network, and PC3 cannot access IP Network.

Network Topology

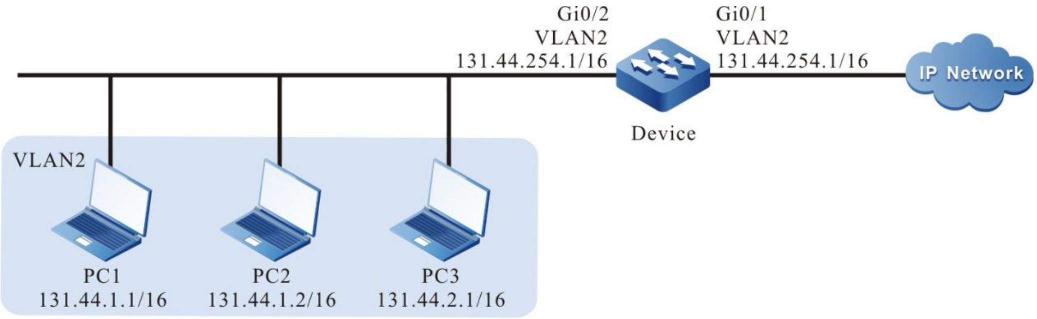


Figure 62–2 Networking of Configuring IP Extended ACL with Time Domain

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1, gigabitethernet0/2 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the corresponding VLAN interface and IP address on Device. (Omitted)

Step 3: Configure the time domain.

#Configure the time domain “time-range-work” on Device and the range is 08:00 to 18:00 every day.

```
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00 to 18:00
Device(config-time-range)#exit
```

#View the current system time on Device.

```
Device#show clock

UTC FRI APR 05 15:26:31 2013
```

#View the information of the defined time domain “time-range-work” on Device.

```
Device#show time-range time-range-work
Timerange name:time-range-work  (STATE:active)
  10  periodic daily 08:00 to 18:00 (active)
```

Step 4: Configure the IP extended ACL.

#Configure the IP extended ACL with serial number 1001 on Device.

```
Device(config)#ip access-list extended 1001
```

#Configure the rule, preventing the network segment 131.44.2.0/24 from accessing IP Network.

```
Device(config-ext-nacl)#deny ip 131.44.2.0 0.0.0.255 any
```

#Configure the rule, permitting PC2 to access the FTP service of IP Network.

```
Device(config-ext-nacl)#permit tcp host 131.44.1.2 any eq ftp
Device(config-ext-nacl)#permit tcp host 131.44.1.2 any eq ftp-data
```

#Configure the rule, permitting PC1 to access IP Network in the defined time domain “time-range-work” range.

```
Device(config-ext-nacl)#permit ip host 131.44.1.1 any time-range time-range-work
Device(config-ext-nacl)#exit
```

#View the information of the ACL with serial number 1001 on Device.

```
Device#show ip access-list 1001
ip access-list extended 1001
 10 deny ip 131.44.2.0 0.0.0.255 any
 20 permit tcp host 131.44.1.2 any eq ftp
 30 permit tcp host 131.44.1.2 any eq ftp-data
 40 permit ip host 131.44.1.1 any time-range time-range-work (active)
```

Step 5: Configure applying the IP extended ACL.

#Apply the IP extended ACL with serial number 1001 to the egress of port gigabitethernet0/1 on Device.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1001 out
Device(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
fa0/1                   OUT          IP         1001
```

Step 6: Check the result.

#PC1 can access IP Network from 08:00 to 18:00 of every day; PC2 can access any FTP server in IP Network; PC3 cannot access IP Network.

62.3.3 Configure MAC Standard ACL *-B -S -E -A*

Network Requirements

- PC1, PC2, and PC3 are connected to IP Network via Device.
- Configure the MAC standard ACL rule, realizing that PC1 can access IP Network, PC2 and PC3 cannot access IP Network.

Network Topology

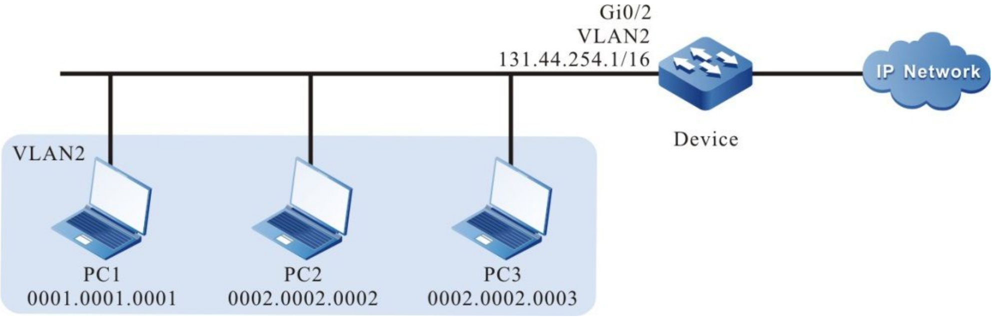


Figure 62–3 Networking of Configuring MAC Standard ACL

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/2 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure the corresponding VLAN interface and IP address on Device. (Omitted)

Step 3: Configure the MAC standard ACL.

#Configure the MAC standard ACL with serial number 2001 on Device.

```
Device(config)#mac access-list standard 2001
```

#Configure the rule, permitting PC1 to access IP Network.

```
Device(config-std-mac-nacl)#permit host 0001.0001.0001
```

#Configure the rule, preventing the network segment with MAC address 0002.0002.0000 and mask ffff.ffff.0000 from accessing IP Network.

```
Device(config-std-mac-nacl)#deny 0002.0002.0000 0000.0000.ffff
```

#View the information of the ACL with serial number 2001 on Device.

```
Device#show mac access-list 2001
mac access-list standard 2001
 10 permit host 0001.0001.0001
 20 deny 0002.0002.0000 0000.0000.ffff
```

Step 4: Configure applying MAC standard ACL.

#Apply the MAC standard ACL with serial number 2001 to the ingress of the port gigabitethernet0/2 on Device.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac access-group 2001 in
Device(config-if-gigabitethernet0/2)#exit
```

#View the information of the ACL applied to the port on Device.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/2                  IN          MAC        2001
```

Step 5: Check the result.

#PC1 can access IP Network; PC2 and PC3 cannot access IP Network.

62.3.4 Configure MAC Extended ACL *-B -S -E -A*

Network Requirements

- PC1, PC2, and IP Phone are connected to IP Network via Device.
- Configure the MAC extended ACL rule on Device2, realizing that the user of VLAN2 cannot access IP Network, and except for the voice users, the other users of VLAN3 all can access IP Network.

Network Topology

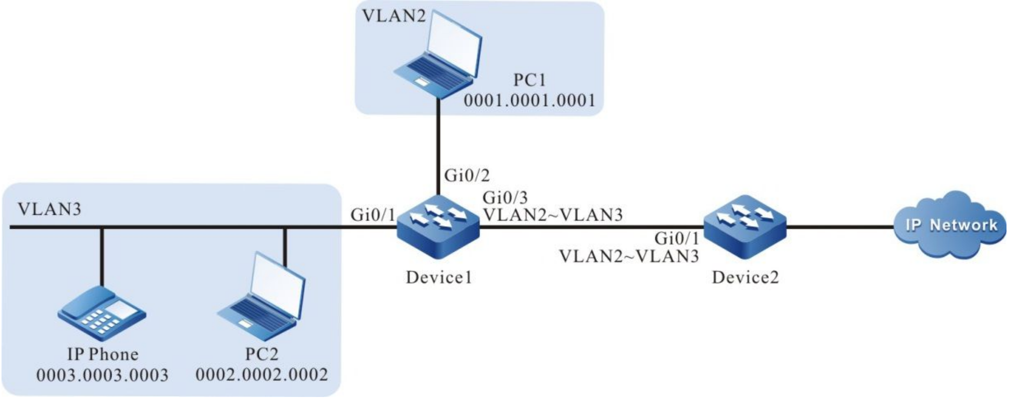


Figure 62–4 Networking of Configuring the MAC Extended ACL

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device2.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the corresponding VLAN interface and IP address on Device1 and Device2. (Omitted)

Step 3: Configure Voice-VLAN to set the COS value of the packet from IP Phone as 7 on Device1. (Omitted)

Step 4: Configure the MAC extended ACL.

#Configure the MAC extended ACL with serial number 3001 on Device2.

```
Device2(config)#mac access-list extended 3001
```

#Configure the rule, preventing the users in VLAN2 from accessing IP Network.

```
Devic2(config-ext-mac-nacl)#deny any any vlan-id 2
```

#Configure the rule, preventing the voice users in VLAN3 from accessing IP Network.

```
Device2(config-ext-mac-nacl)#deny any any cos 7 vlan-id 3
```

#Configure the rule, permitting the other users in VLAN3 to access IP Network.

```
Device2(config-ext-mac-nacl)#permit any any vlan-id 3
```

#View the information of the ACL with serial number 3001 on Device2.

```
Device2#show access-list 3001
mac access-list extended 3001
 10 deny any any vlan-id 2
 20 deny any any cos 7 vlan-id 3
 30 permit any any vlan-id 3
```

Step 5: Configure applying the MAC extended ACL.

#Apply the MAC extended ACL with serial number 3001 to the ingress of the port gigabitethernet0/1 on Device2.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#mac access-group 3001 in
Device2(config-if-gigabitethernet0/1)#exit
```

#View the information of the ACL applied to the port on Device2.

```
Device2#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1                    IN           MAC        3001
```

Step 6: Check the result.

#PC2 can access IP Network; PC1 and IP Phone cannot access IP Network.

NOTE

- For the configuration of Voice-VLAN, refer to the Voice-VLAN chapter of the configuration manual.

62.3.5 Configure Hybrid Extended ACL *-B -S -E -A*

Network Requirements

- PC1, PC2, and PC3 are connected to IP Network via Device.
- Configure the Hybrid extended ACL rule, realizing that PC1 can access IP Network within the specified time, PC2 and PC3 cannot access IP Network.

Network Topology

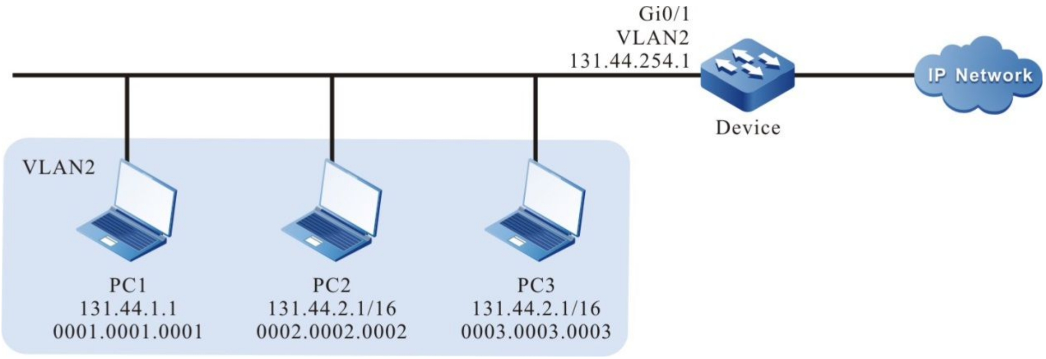


Figure 62–5 Networking of Configuring Hybrid Extended ACL

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the corresponding VLAN interface and IP address on Device. (Omitted)

Step 3: Configure the time domain.

#Configure the time domain “time-range-work” on Device and the range is 08:00 to 18:00 every day.

```
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00 to 18:00
Device(config-time-range)#exit
```

#View the current system time on Device.

```
Device#show clock

UTC FRI APR 05 15:26:31 2013
```

#View the information of the defined time domain “time-range-work” on Device.

```
Device#show time-range time-range-work
Timerange name:time-range-work  (STATE:active)
  10  periodic daily 08:00 to 18:00 (active)
```

Step 4: Configure the Hybrid extended ACL list.

#Configure the Hybrid extended ACL with serial number 5001 on Device.

```
Device(config)#hybrid access-list extended 5001
```

#Configure the rule, preventing the network segment 131.44.2.0/24 from accessing IP Network.

```
Device(config-hybrid-nacl)#deny ip 131.44.2.0 0.0.0.255 any
```

#Configure the rule, permitting PC1 to access IP Network in the defined time domain “time-range-work” range.

```
Device(config-hybrid-nacl)#permit ip host 0001.0001.0001 time-range time-range-work
```

#Configure the rule, permitting all packets from IP Network to pass Device.

```
Device(config-hybrid-nacl)#permit ip any any
Device(config-hybrid-nacl)#exit
```

#View the information of the ACL with serial number 5001 on Device.

```
Device#show hybrid access-list 5001
hybrid access-list extended 5001
 10 deny ip 131.44.2.0 0.0.0.255 any
 20 permit ip any host 0001.0001.0001 time-range time-range-work (active)
 30 permit ip any any
```

Step 5: Configure applying Hybrid extended ACL.

#Apply the Hybrid extended ACL with serial number 5001 to the ingress globally.

```
Device(config)#global hybrid access-group 5001 in
```

#View the information of the ACL applied globally on Device.

```
Device#show acl-object global
```

```
----------------Global-----Bind-----Instance-----------
Global-------------------Direction----AclType----AclName
global                   IN           HYBRID     5001
```

Step 6: Check the result.

#PC1 can access IP Network from 08:00 to 18:00 every day; PC2 and PC3 can access IP Network.

63 URPF

63.1 URPF Overview

Nowadays in Internet, many cyber attacks are attacking messages sent from spoofed source IP addresses. The use of spoofed addresses is out of the attacker's concern with traceability of his/her own IP address. On the other hand, some attacks like Land and Smurf have message source IP addresses identical to the attacked IP addresses. In order to limit the damages caused by attacks from spoofed source addresses and trace the attack source, it is proposed in rfc2827, rfc3704 that filtering of traffics from spoofed source IP addresses shall be carried out by ISP or at edge devices. This is an idea to suppress attacks at their message sources.

The major function of URPF (Unicast Reverse Path Forwarding) is to prevent spoofed source address based cyber attacks, that is, to find out the attacking messages' source addresses by searching reverse routing tables during the forwarding process of the messages in order to determine whether or not to forward them according to the searching results. This strategy can effectively prevent attacks based on IP address spoofing, especially DoS attacks from spoofed source IP addresses. URPF check can be done in either strict mode or loose mode.

Cyber attacks constitute a serious threat to cyber security. URPF is an effective method to defend against cyber attacks. It aims to filter cyber attack messages from spoofed source IP addresses at ISP or at edge devices, in order to limit the damage caused by cyber attack messages in early stage.

63.2 Configuration of URPF Function

Table 63-1 Functional Configuration List of UPPF

Configuration task	
Configure URPF function	Configure URPF check

63.2.1 Configure URPF Function *-E -A*

Configuration Conditions

N/A.

Configure URPF Check

The configuration of URPF check is for filtering spoofed IP addresses based attacking messages at receiving interfaces. URPF supports checks in strict mode or loose mode. In loose mode, URPF will perform routing table search of the source address of received messages. If the routing information of the messages can be found, the messages will be forwarded. In strict mode, the messages will be forwarded only when their routing is identified and their outgoing interface coincides with their receiving interface.

Table 63-2 Configure URPF Check

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Turn on global URPF check	**ip urpf [allow-default-route]**	Required
Enter the interface configuration mode	**interface** *interface-name*	-
Turn on port URPF check	**ip urpf** { **loose | strict** }	Required By default, port URPF check is not turned on. Interface URPF check is activated only after global URPF check is enabled.

63.2.2 URPF Monitoring and Maintenance *-E -A*

Table 63-3 URPF Monitoring and Maintenance

Command	Description
show ip urpf brief	Display interface URPF configuration information
show ip urpf config	Display global and interface URPF configuration information

63.3 Example of URPF Typical Configuration

63.3.1 Configure URPF Strict Mode *-E -A*

Network requirements

- PC accesses IP network via Device, and the Device has been configured URPF in strict mode.
- The PC that simulates an attacker sends illegal message with pseudo source address to access IP network, and the device's URPF function discards the message.

Network topology

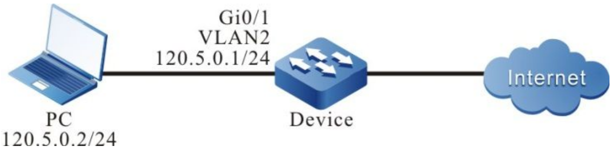


Figure 14-63-1 Networking Diagram - Configure URPF Strict Mode

Configuration steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP addresses and routing for the interfaces, requiring that PC can access IP Network via device (omitted)

Step 3: Configure URPF strict mode.

#On the Device, enable URPF function, and on interface vlan2 configure URPF strict mode.

```
Device#configure terminal
Device(config)#ip urpf
Device(config)#interface vlan2
Device(config-if- vlan2)#ip urpf strict
Device(config-if- vlan2)#exit
```

Step 4: Check the result.

#PC accesses IP Network via Device, source address is 120.5.0.2.

Device has routing to 120.5.0.2, the routing outgoing interface is VLAN2. If the routing outgoing interface to source address is the same interface VLAN2 with the receiving interface of the message, the message will pass URPF check in strict mode and will be forwarded by the device. As a result, the PC will be able to access the IP network.

#The PC that simulates an attacker sends illegal messages with pseudo (spoofed) source address, and accesses the IP network via Device, the source address is 120.10.0.2.

Device has no routing to 120.10.0.2, URPF discards the message, the PC cannot access IP Network.

63.3.2 Configure URPF Loose Mode *-E -A*

Network requirements

- In network environment, PC1 accesses PC2 via Device1, Device2, Device3, PC2's response message reaches PC1 via Device3, Device1.
- On Device3, configure URPF loose mode.

- PC1 that simulates an attacker sends illegal message with pseudo source address to access PC2, Device3's URPF function discards the message.

Network topology

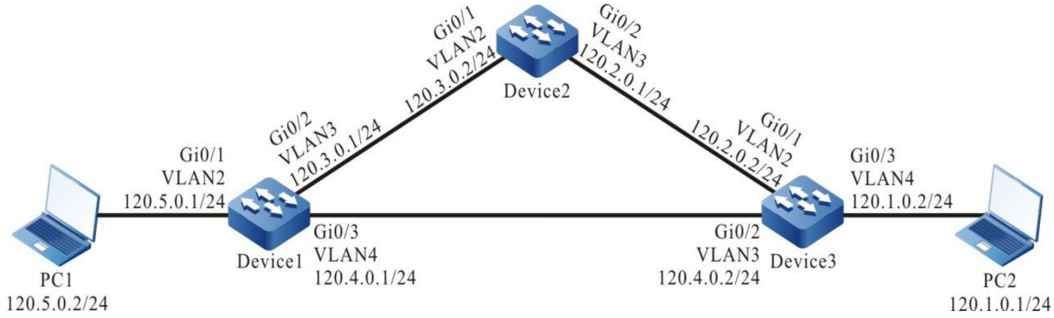


Table 14-63-2 Networking Diagram - Configure URPF Loose Mode

Configuration steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure the interfaces' IP addresses. (omitted)

Step 3: Configure static routing in network, so that PC1 accesses PC2 via Device1, Device2, Device3, PC2's response message reaches PC1 via Device3, Device1.

#Configure Device1, Device2, Device3's static routing, construct network environment specified in network requirements.

```
Device1#configure terminal
Device1(config)#ip route 120.1.0.0 255.255.255.0 120.3.0.2
Device1(config)#ip route 120.2.0.0 255.255.255.0 120.3.0.2

Device2#configure terminal
Device2(config)#ip route 120.1.0.0 255.255.255.0 120.2.0.2

Device3#configure terminal
Device3(config)#ip route 120.5.0.0 255.255.255.0 120.4.0.1
```

#Check Device1, Device2, Device3's routing table .

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

S   120.1.0.0/24 [1/10] via 120.3.0.2, 00:10:49, vlan3
S   120.2.0.0/24 [1/10] via 120.3.0.2, 00:11:19, vlan3
C   120.3.0.0/24 is directly connected, 00:19:15, vlan3
C   120.4.0.0/24 is directly connected, 00:15:00, vlan4
C   120.5.0.0/24 is directly connected, 00:07:36, vlan2
C   127.0.0.0/8 is directly connected, 357:23:02, lo0

Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

S   120.1.0.0/24 [1/10] via 120.2.0.2, 00:15:37, vlan3
C   120.2.0.0/24 is directly connected, 00:17:17, vlan3
C   120.3.0.0/24 is directly connected, 00:25:21, vlan2
```

```
C   127.0.0.0/8 is directly connected, 00:38:29, lo0

Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   120.1.0.0/24 is directly connected, 00:17:01, vlan4
C   120.2.0.0/24 is directly connected, 00:19:13, vlan2
C   120.4.0.0/24 is directly connected, 00:18:50, vlan3
S   120.5.0.0/24 [1/10] via 120.4.0.1, 00:17:19, vlan3
C   127.0.0.0/8 is directly connected, 00:26:16, lo0
```

Step 4: Configure URPF loose mode on Device3.

#On Device3, enable URPF function, and on vlan interface2 configure URPF loose mode.

```
Device3#configure terminal
Device3(config)#ip urpf
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ip urpf loose
Device3(config-if-vlan2)#exit
```

Step 5: Check the result.

#PC1 ping PC2

PC1's ping request message reaches PC2 via Device1, Device2, and Device3; PC2's ping response message reaches PC1 via Device3, Device1.

#PC1 accesses PC2, source address is 120.5.0.2.

Device3 has routing to 120.5.0.2, the routing outgoing interface is VLAN3. The routing outgoing interface VLAN 3 to source address and the message's receiving interface VLAN 2 are not the same interface, however, the message has passed URPF check in loose mode and is forwarded by Device3. As a result, PC1 can access PC2 and PC2's response message reaches PC1 via Device3, Device1.

#PC1 that simulates an attacker sends illegal messages with pseudo (spoofed) source address to access PC2, the source address is 120.10.0.2.

Device3 has no routing to 120.10.0.2, URPF discards the message, PC1 cannot access PC2.

NOTE

- Messages discarded as a result of this detection will generate neither logs nor statistical information.
- The difference between strict mode URPF and loose mode URPF is that: in loose mode, URPF will search routing table for the source IP address of the received message; if the routing is found, the message will be forwarded; in strict mode, the message will be forwarded only when its routing is found and its outgoing interface coincides with the message's receiving interface.
- Generally strict mode is used. Loose mode is used in network environment featuring "inconsistent consistent round-trip path” and the like.

64 Attack Detection

64.1 Overview

The attack detection is one important function of maintaining the network security. It analyzes the packet content processed by the device, judges whether the packet has the attack feature and executes some precautions for the packet with the attack feature according to the configuration, such as intercept the attack packet and record the attack packet log. Configuring the attack detection function on the device, on one hand, can avoid that the device becomes abnormal because of getting the network attack, improving the anti-attack capability of the device; on the other hand, it can intercept the attack traffic forwarded by the device, avoiding that the other devices on the network cannot work normally because of being attacked.

64.2 Attack Detection Function Configuration

Table 64-1 The configuration List of the Attack Detection Function

Configuration Task	
Configure the software attack detection function	Configure intercepting the packet with too small IP length
	Configure intercepting the unreasonable fragment packets
	Configure intercepting the Land attack packet
	Configure intercepting the Smurf attack packet
	Configure intercepting the Fraggle attack packet
	Configure intercepting the ICMP flood attack packet
	Configure intercepting the TCP SYN flood attack packet
	Configure the software attack detection log recording

Configuration Task	
Configure the hardware attack detection function	Configure intercepting the packet with the same source and destination MAC
	Configure intercepting the packet with the same source and destination IP
	Configure intercepting the TCP packet with the same source and destination port
	Configure intercepting the UDP packet with the same source and destination port
	Configure intercepting the invalid TCP packet
	Configure intercepting the invalid ICMP packet
	Configure intercepting the TCP SYN packet with the source port smaller than 1024

NOTE

- The software attack detection function is valid only for the packet to the local device; the hardware attack detection function is valid for all the packets received by the switching port.
- The software attack detection supports the statistics and log recording for the dropped packers; the hardware attack detection is realized by the switching chip and does not support the statistics and log recording for the dropped packets.

64.2.1 Configure Software Attack Detection Function *-B -S -E -A*

The software attack detection function is realize by adopting the software mode, performing the attack detection only for the packet with the destination address as the device itself, so as to prevent the device from getting the network attack.

Configuration Conditions

Before configuring intercepting the Smurf, Fraggle, ICMP flood, and TCP SYN flood attack detection functions, first complete the following tasks:

- Configure ACL

Configure Intercepting Packet with Too Small IP Length

When the device receives the IP packet with the IP length (including the IP head and load) smaller than the configured length, drop the packet.

Table 64-2 Configure Intercepting the Packet with Too Small IP Length

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the packet with too small IP length	**ip intercept small-packet** [*length*]	Mandatory By default, do not configure the function of intercepting the packet with too small IP length. After configuring the function and if not specifying the length, intercept the packet with the IP length smaller than 64 bytes by default.

Configure Intercepting Unreasonable Fragment Packet

When the device receives the IP fragment packet and the fragment offset plus its own load length exceeds the configured length, drop the packet.

Table 64-3 Configure Intercepting Unreasonable Fragment Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting unreasonable fragment packet	**ip intercept fragment** [**max-off** *length*]	Mandatory By default, do not configure the function of intercepting the unreasonable fragment packet. After configuring the function and if not specifying the length, intercept the fragment whose offset plus its own load length exceeds 65535 by default.

Configure Intercepting Land Attack Packet

Land attack adopts the same source and destination IP and port to send the TCP SYN packet to the target machine, making the target system with the hole create one TCP empty connection with itself, even resulting in the breakdown of the target system.

When the device receives the TCP SYN packet with the same source and destination IP and the same source and destination port, drop the packet.

Table 64-4 Configure Intercepting the Land Attack Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the Land attack packet	**ip tcp intercept land**	Mandatory By default, do not configure intercepting the Land attack packet.

Configure Intercepting Smurf Attack Packet

The Smurf attack sends the ICMP request packet to one network and the destination IP is the subnet broadcast address of the network. As a result, all hosts of the network answer the ICMP request. Therefore, the network of the source IP is blocked and the source IP host is busy with processing the ICMP responses.

When the device receives the ICMP packet and if the ICMP type is ICMP_ECHO, ICMP_TSAMP, ICMP_MASKREQ or ICMP_IREQ and the destination IP is the subnet broadcast address, the packet is regarded as the Smurf attack packet and is dropped.

Table 64-5 Configure Intercepting Smurf Attack Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting Smurf attack packet	**ip smurf intercept list** { *access-list-number* | *access-list-name* } [**masklen** *length*]	Mandatory By default, do not configure the function of intercepting the Smurf attack packet. After configuring the function and if not specifying the mask length, the mask length is 24 by default.

NOTE

- When configuring intercepting the Smurf attack packet, first need to create the ACL, used to specify the protected data flow. We check whether it is the Smurf attack packet only for the data flow permitted by the ACL. Otherwise, permit the packet to pass.
- **masklen** *length* in the configuration command is used to specify the mask length; when the last bit of the destination IP (32-mask length) is 1, it is regarded as the subnet broadcast address.

Configure Intercepting Fraggle Attack Packet

The Fraggle attack is similar to the Smurf attack and it makes use of the UDP packet to attack.

When the device receives the UDP packet and the destination IP is the subnet broadcast address, it is regarded as the Fraggle attack packet and is dropped.

Table 64-6 Configure Intercepting the Fraggle Attack Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the Fraggle attack packet	**ip fraggle intercept list** { *access-list-number* | *access-list-name* } [**masklen** *length*]	Mandatory By default, do not configure the function of intercepting the Fraggle attack packet. After configuring the function and if not specifying the mask length, the mask length is 24 by default.

NOTE

- When configuring intercepting the fraggle attack packet, first need to create the ACL, used to specify the protected data flow. We check whether it is the fraggle attack packet only for the data flow permitted by the ACL. Otherwise, permit the packet to pass.
- **masklen** *length* in the configuration command is used to specify the mask length; when the last bit of the destination IP (32-mask length) is 1, it is regarded as the subnet broadcast address.

Configure Intercepting ICMP Flood Attack Packet

ICMP flood attack sends lots of ICMP response requests to the target host to make the network of the target host be blocked. The target host consumes lots of resources to answer and cannot provide services normally.

When the number of the ICMP packets with the same destination IP received by the device within one second exceeds the threshold, the packets exceeding the threshold are dropped.

Table 64-7 Configure Intercepting the ICMP Flood Attack Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the ICMP flood attack packet	**ip icmp intercept list** { *access-list-number* | *access-list-name* } [**maxcount** *number*]	Mandatory By default, do not configure the function of intercepting the ICMP flood attack packet. After configuring the function and if not specifying the threshold, the default value is 500.

NOTE

- When configuring intercepting the ICMP flood attack packet, first need to create the ACL, used to specify the protected data flow. We check whether it is the ICMP flood attack packet only for the data flow permitted by the ACL. Otherwise, permit the packet to pass.

Configure Intercepting TCP SYN Flood Attack Packet

TCP SYN Flood attack sends lots of TCP SYN requests to the target host, but does not answer the ACK message. As a result, the target host has lots of semi-connections waiting for receiving the ACK message of the requester, which occupy the available resources of the target host. As a result, the target host cannot provide the normal network services.

When the number of the TCP SYN packets with the same destination IP received by the device within one second exceeds the threshold, the packets exceeding the threshold are dropped.

Table 64-8 Configure Intercepting the TCP SYN Flood Attack Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the TCP SYN flood attack packet	**ip tcp intercept list** { *access-list-number* | *access-list-name* } [**maxcount** *number*]	Mandatory By default, do not configure the function of intercepting the TCP SYN flood attack packet. After

Step	Command	Description
		configuring the function and if not specifying the threshold, the default value is 500.

NOTE

- When configuring intercepting the TCP SYN flood attack packet, first need to create the ACL, used to specify the protected data flow. We check whether it is the TCP SYN flood attack packet only for the data flow permitted by the ACL. Otherwise, permit the packet to pass.

Configure Intercepting Address and Port Scanning Attack Packet

The address scanning attack means that the attacker sends the CMP packets to detect the active host on the network, while the port scanning means that the attacker sends the TCP or UDP packet to detect the enabled port of the active host on the network. With the address and port scanning, the attacker can get the active host information on the network. Usually, the address and port scanning is the omen of the attacker initiating the network attack.

When the number of the ICMP packets with the same IP and different destination IPs received by the device within one second exceeds the threshold, it is regarded as the address scanning attack and the packets exceeding the threshold are dropped. When the number of the TCP or UDP packets with the same source IP and different destination ports received by the device within on second exceeds the threshold, it is regarded as the port scanning attack and the packets exceeding the threshold are dropped.

Table 64-9 Configure Intercepting the Address and Port Scanning Attack Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interfa**ce *interface-name*	-
Configure intercepting the address and port scanning attack packet	**scanprotect** { **default |** **interval** { **default |** *interval-value* } **addr-limit** { **default** | *max-addr-value* } **port-limit** { **default** | *max-port-value* } **ban-timeout** { **default** | *max-ban-timeout* } }	Mandatory By default, do not configure the function of intercepting the address and port scanning attack packets. After configuring the function, the default interval is 1s, the default address scanning

Step	Command	Description
		threshold is 10 different IPs, and the default port scanning threshold is 10 different destination ports.

Configure Software Attack Detection Log Recording

When the device software attack detection intercepts the attack packet, record the log information.

Table 64-10 Configure the Software Attack Detection Log Recording

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the software attack detection log recording	**ip intercept log**	Mandatory By default, do not configure the software attack detection log function.

64.2.2 Configure Hardware Attack Detection Function *-B -S -E -A*

Configuration Conditions

None

Configure Intercepting Packet with Same Source and Destination MAC

When the switching port of the device receives the packet with the same source and destination MAC, drop the packet.

Table 64-11 Configure Intercepting the Packet with the Same Source and Destination MAC

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the packet with the same source and destination MAC	**ip mac intercept bad**	Mandatory By default, do not configure the function of intercepting the packet

Step	Command	Description
		with the same source and destination MAC

Configure Intercepting Packet with Same Source and Destination IP

When the switching port of the device receives the packet with the same source and destination IP, drop the packet.

Table 64-12 Configure Intercepting the Packet with the Same Source and Destination IP

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the packet with the same source and destination IP	**ip intercept ipeq**	Mandatory By default, do not configure the function of intercepting the packet with the same source and destination IP.

Configure Intercepting TCP Packet with Same Source and Destination Port

When the switching port of the device receives the TCP packet with the same source and destination port, drop the packet.

Table 64-13 Configure Intercepting the TCP Packet with the Same Source and Destination Port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the TCP packet with the same source and destination port	**ip tcp intercept porteq**	Mandatory By default, do not configure the function of intercepting the TCP packet with the same source and destination port.

Configure Intercepting UDP Packet with Same Source and Destination Port

When the switching port of the device receives the UDP packet with the same source and destination port, drop the packet.

Table 64-14 Configure Intercepting the UDP Packet with the Same Source and Destination Port

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the UDP packet with the same source and destination port	**ip udp intercept porteq**	Mandatory By default, do not configure the function of intercepting the UDP packet with the same source and destination port.

Configure Intercepting Invalid TCP Packet

When the switching port of the device receives the invalid TCP packet, drop the packet.

The packet with any one of the following features is regarded as the invalid TCP packet. The features are as follows:

1. The TCP head length of the first fragmented packet is smaller than the configured value;
2. The flags and sequence number fields in the TCP head are both equal to 0;
3. The SYN and FIN in the flags field of the TCP head are set at the same time;
4. FIN, URG, and PSH in the flags field of the TCP head are set at the same time and the sequence number field is equal to 0;
5. The TCP fragment packet with the offset 1.

Table 64-15 Configure intercepting the invalid TCP packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the invalid TCP packet	**ip tcp intercept bad** [*length*]	Mandatory By default, do not configure the function of intercepting the invalid TCP packet.

Configure Intercepting Invalid ICMP Packet

When the switching port of the device receives the invalid ICMP packet, drop the packet.

The packet with any one of the following features is regarded as the invalid ICMP packet. The features are as follows:

1. The fragmented ICMP packet
2. ICMP ping packet and the length exceeds the configured value.

Table 64-16 Configure Intercepting the Invalid ICMP Packet

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the invalid ICMP packet	**ip icmp intercept bad** [**length** *value*]	Mandatory By default, do not configure the function of intercepting the invalid ICMP packet.

Configure TCP SYN Packet with Source Port Smaller than 1024

When the switching port of the device receives the TCP SYN packet and the TCP source port is smaller than 1024, drop the packet.

Table 64-17 Configure Intercepting the TCP SYN Packet with the Source Port Smaller than 1024

Step	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure intercepting the TCP SYN packet with the source port smaller than 1024	**ip tcp intercept sport-limit**	Mandatory By default, do not configure the function of intercepting the TCP SYN packet with the source port smaller than 1024.

64.2.3 Monitoring and Maintaining of Attack Detection *-B -S -E -A*

Table 64-18 Attack Detection Monitoring and Maintaining

Command	Description
clear ip intercept statistic	Clear the software attack detection statistics information
show ip intercept config	Display the attack detection configuration information
show ip intercept statistic	Display the software attack detection statistics information
show scanprotect config	Display the scanning attack detection configuration information
show scanprotect monitor	Display the scanning attack detection statistics information
clear scanprotect	Clear the scanning attack check statistics information

64.3 Typical Configuration Example of Attack Detection

64.3.1 Configure Anti-DDOS Attack Detection *-B -S -E -A*

Network Requirements

- Device is connected to IP Network via port gigabitethernet0/1.
- Device configures the anti-DDOS attack detection function. When finding the attack packet, alarm and drop the attack packet, taking the common SYN Flood attack, Smurf attack, and Land attack as example.

Network Topology

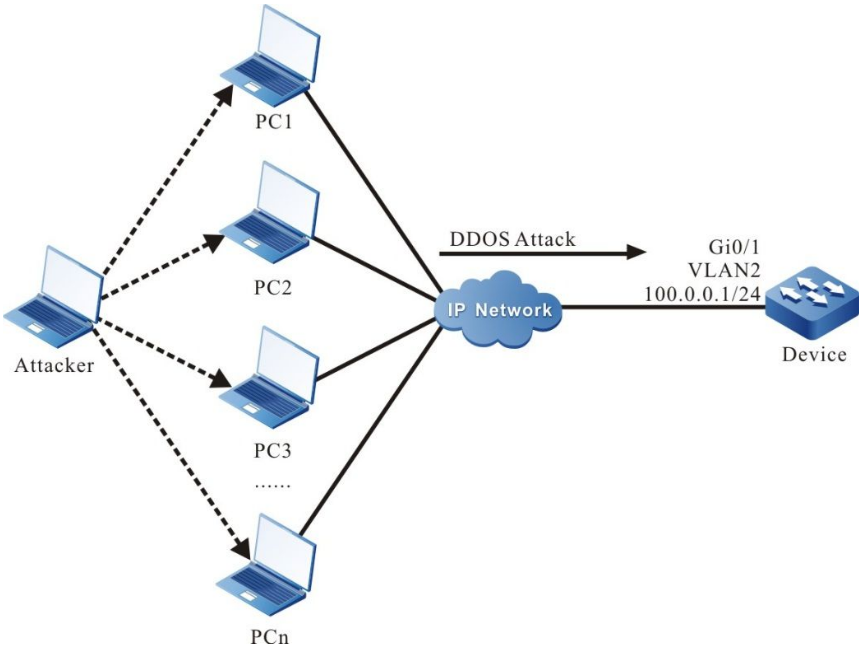


Figure 64-1 Networking of Configuring the anti-DDOS Attack Detection

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the ACL rule.

#Configure the standard ACL rule, matching the Device address to be protected.

```
Device#configure terminal
Device(config)#ip access-list standard 1
Device(config-std-nacl)#permit host 100.0.0.1
Device(config-std-nacl)#exit
```

Step 4: Configure the attack detection function and enable the log recording function.

#Configure the SYN Flood, Smurf, and Land attack detection function on Device.

```
Device(config)#ip tcp intercept list 1
Device(config)#ip smurf intercept list 1
Device(config)#ip tcp intercept land
```

#Enable the anti-DDOS attack detection log recording function on Device.

```
Device(config)#ip intercept log
```

Step 5: Check the result.

#When Device gets the SYN Flood attack, output the following log information:

```
%FIREWALL-FLOOD_WARN-4: vlan2 gigabitethernet0/1 SYN flood attack detected, destination IP 100.0.0.1,
1000 packets/second.
```

#When Device gets the Smurf attack, output the following log information:

```
%FIREWALL-SMURF_WARN-4: SMURF attack detected at vlan2 gigabitethernet0/1, source IP 100.0.0.1,
destination IP 100.0.0.255, icmp type 8.
```

#When Device gets the Land attack, output the following log information:

```
%FIREWALL-LAND_WARN-4: LAND attack detected at vlan2 gigabitethernet0/1, source IP equal destination
IP is 100.0.0.1, source port equal destination port is 1024.
```

#View the attack detection packet statistics information on Device:

```
Device#show ip intercept statistic
IP intercept        Drops
-------------------- ----------
Small IP            0
Fragment            0
Land                6256
Smurf               4893
Fraggle             0
SYN Flood           6200
ICMP Flood          0
```

NOTE

- The DDOS attack detection function is valid only for the packets processed by CPU.

64.3.2 Configure Intercepting Attack with Same Source and Destination IP Address

-B -S -E -A

Network Requirements

- Device configures the detection function of intercepting the attack with the same source and destination IP address, detecting the attack packet and dropping it.

Network Topology

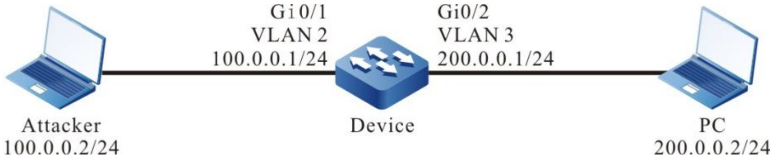


Figure 64–2 Networking of Configuring Intercepting the Attack with the Same Source and Destination IP Address

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the attack detection function.

#Configure the detection function of intercepting the attack with the same source and destination IP address.

```
Device#configure terminal
Device(config)#ip intercept ipeq
```

Step 4: Check the result.

#When Attacker initiates the packet attack with the same source and destination IP address to PC, we cannot capture the attack packet on PC.

NOTE

- The detection function of intercepting the attack with the same source and destination IP address is valid for the packets processed by CPU and the service packets.
- When the detection function of intercepting the attack with the same source and destination IP address drops the packet, do not generate the log or statistics information.

65 HA

65.1 Overview

HA (High Availability) is one high availability management platform on the device and mainly includes the hot-swap function of the device service card and the hot-swap function of the power. Besides, it provides the regular detection for some system faults, ensuring that the services are not interrupted.

The hot-swap function of the service card means to swap via the command and also can directly swap manually, so as to meet the different requirements of the user. When the same slot is inserted the same service card as the previous one, the configuration on the service card automatically recovers; when the same slot is inserted with one service card different from the previous one, the configuration is restored to the empty configuration.

The hot-swap function of the power means that the user can swap the power manually. The function is to ensure that the power can be pulled out without affecting the normal work of the system when the system power fault needs to be fixed. Besides, when the device needs to add power, insert the new parts and start to work when the system works normally. Note that the operations need to be realized according to the correct operation mode.

65.2 HA Function Configuration

Table 65–1 HA Function Configuration List

Configuration Task	
The hot-swap function of the service card	Hot-swap the service card
The hot-swap function of the power	The hot-swap function of the power

65.2.1 HA Monitoring and Maintaining *-B -S -E -A*

Table 65–2 HA Monitoring and Maintaining

Command	Description
show ham job	Display the HA task processing node table of the local device

66 ULFD

66.1 Overview

In the traditional Ethernet, we usually use the fiber and other physical medium to connect the devices. In the actual networking, the fiber crossover connection (Figure 2-1), or one fiber not connected or disconnected (Figure 2-2) may result in the uni-directional communication. This kind of faulty link is called uni-directional link. The uni-directional link causes a series of problems. For example, the STP detection failure results in the topology calculation error.

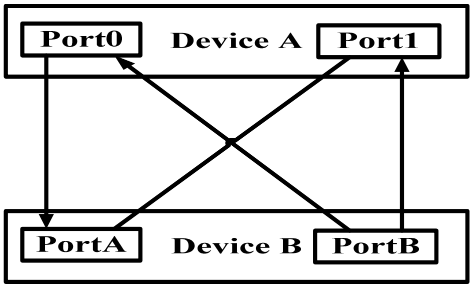


Figure 66-1 Fiber Crossover Connection

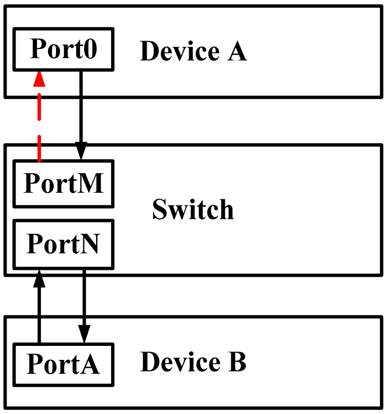


Figure 66-2 One Fiber is not Connection or Disconnected

ULFD (Unidirectional Link Fault Detection) can monitor whether the fiber or twisted-pair has the uni-directional link. When ULFD detects the uni-directional link, it is responsible for closing the physical and logical uni-directional connection, sending the alarm information to the user and blocking the failure of other protocols.

66.2 ULFD Function Configuration

Table 66–1 ULFD Function Configuration List

Configuration Task	
Configure the ULFD basic functions	Enable global ULFD function
	Enable the port ULFD function
Configure the ULFD parameters	Configure the period of sending the ULFD detection packets
	Re-set the port disabled by ULFD

66.2.1 Configure ULFD Basic Functions *-B -S -E -A*

Configuration Conditions

Before configuring the ULFD basic functions, first complete the following task:

- Ensure that the ULFD detection port is connected normally

Enable Global ULFD Function

ULFD has two work modes, that is, normal and aggressive. For the two modes, the basis of judging the uni-directional link is different. The normal mode is often used to check the uni-direction caused by the crossover connection. The aggressive mode is used to check the uni-directional connection caused by the crossover connection or disconnection.

Table 66–2 Enable Global ULFD Function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable global ULFD function	**ulfd** { **aggressive** | **enable** }	Mandatory By default, do not enable global ULFD function.

Enable the Port ULFD Function

ULFD detection needs to enable the global ULFD detection function and the port ULFD detection function. If the ULFD function is not enabled globally, but just enabled on the port, the ULFD function cannot take effect.

If the global enabled ULFD detection mode and port enabled ULFD detection mode are inconsistent, the port ULFD detection mode takes effect first.

Table 66–3 Enable the Port ULFD Function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Enable the port ULFD function	**ulfd port** [**aggressive**]	Mandatory By default, do not enable the port ULFD function.

NOTE

- To switch over the ULFD work mode on the port, first cancel the previous work mode and then configure the new mode.
- When enabling the ULFD function on the port, ensure that the neighbor port is also configured with the ULFD function and works in the same detection mode.

66.2.2 Configure ULFD Parameters *-B -S -E -A*

Configuration Conditions

Before configuring the ULFD parameters, first complete the following task:

- Enable the ULFD function

Configure Sending Period of ULFD Detection Packet

ULFD periodically sends the detection packets to detect whether the network has the uni-directional link. We can modify the sending period of the detection packets according to the actuality of the network. The sending period of the detection packets is 7-90s. By default, it is 15s.

Table 66–4 Configure the Sending Period of the ULFD Detection Packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-

Step	Command	Description
Configure the sending period of the ULFD packet	**ulfd message time** *time-value*	Optional By default, the sending period of the uni-directional detection packet is 15s.

Reset Port Disabled by ULFD

If ULFD detects the uni-direction and disables the port and we want to re-enable the ULFD detection function of the port, the user needs to perform the reset operation manually. The operation sets the port to UP and re-enables the ULFD detection.

Table 66–5 Reset the Port Disabled by ULFD

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Reset the port disabled by ULFD	**ulfd reset** [**interface** *interface-name*]	Optional By default, do not execute the reset operation automatically after the port is disabled.

66.2.3 ULFD Monitoring and Maintaining *-B -S -E -A*

Table 66–6 ULFD Monitoring and Maintaining

Command	Description
show ulfd [**all** | **interface** *interface-name* [**detail**]]	Display the ULFD global configuration information and all/specified port ULFD configuration information

66.3 ULFD Typical Configuration Example

66.3.1 Configure ULFD Basic Function *-B -S -E -A*

Network Requirements

- Device1 and Device2 are connected via the fiber.
- Configure the ULFD normal mode to disable the port when detecting the uni-directional link.

Network Topology

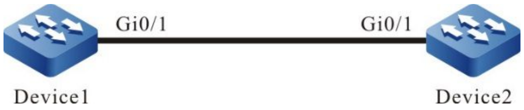


Figure 66-3 Networking of Configuring the ULFD Basic Function

Configuration Steps

Step 1: Configure the ULFD function

#Enable the ULFD function on Device1 and configure the ULFD work mode as the normal mode on port gigabitethernet0/1.

```
Device1#configure terminal
Device1(config)#ulfd enable
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#ulfd port
Device1(config-if-gigabitethernet0/1)#exit
```

#Enable the ULFD function on Device2 and configure the ULFD work mode on port gigabitethernet0/1 as the normal mode.

```
Device2#configure terminal
Device2(config)#ulfd enable
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#ulfd port
Device2(config-if-gigabitethernet0/1)#exit
```

#View the ULFD information of port gigabitethernet0/1 on Device1.

```
Device1#show ulfd interface gigabitethernet 0/1
Interface name      : gigabitethernet0/1
ULFD config mode    : Normal
ULFD running mode   : Normal
Link status         : Link Up
Link direction      : Bidirectional
ULFD fsm status     : Advertisement

Neighbors number    : 1
----------
  Device ID          : 94aee3787878
  Interface name     : gigabitethernet0/1
  Device Name        : Device2
  Message Interval   : 15
  Timeout Interval   : 5
  Link Direction     : Bidirectional
  Aging Time         : 40
  Time to Die        : 36
-------------------------------------
```

NOTE

- The method of viewing the port ULFD information on Device2 is the same as that of Device1. (Omitted)

Step 2: Check the result.

#In the actual networking environment, when the fibers are cross-connected or one fiber is not connected, disconnected, it results in the uni-directional communication. After configuring the ULFD function, port gigabitethernet0/1 is disabled when detecting the uni-directional connection on Device1 and the following log information is output:

```
%ULFD_LOG_WARN: gigabitethernet0/1: detected Unidirectional neighbor: device ID[94aee3787878], device
name[Device2], interface name[gigabitethernet0/1]!
%LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
%ULFD-UNDIR_LINK_ERR_V2-5: ULFD shutdown interface gigabitethernet0/1 successful
```

#View the status of the port gigabitethernet0/1 and we can see that the port is disabled.

```
Device1#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
    Description     :
    Status          : Enabled
    Link            : Down  (Err-disabled)
    Set Speed       : Auto
    Act Speed       : Unknown
    Set Duplex      : Auto
    Act Duplex      : Unknown
    Set Flow Control : Off
    Act Flow Control : Off
    Mdix            : Normal
    Mtu             : 1824
    Port mode       : LAN
    Port ability    : 100M FD,1000M FD
    Link Delay      : No Delay
    Storm Control   : Unicast Disabled
    Storm Control   : Broadcast Disabled
    Storm Control   : Multicast Disabled
    Storm Action    : None
    Port Type       : Nni
    Pvid            : 1
    Set Medium      : Fiber
    Act Medium      : Fiber
    Mac Address     : 0000.1111.2224
```

NOTE

- When configuring the ULFD function, ensure that ULFD configured at the two sides of the link work in the same detection mode.
- When ULFD work mode is aggressive mode, refer to the configuration method.

67 VRRP

67.1 Overview

VRRP (Virtual Router Redundancy Protocol) is one fault tolerance protocol. It ensures that when the next-hop device of the host fails, it can be replaced by another device in time, so as to ensure the continuity and reliability of the communication. To make VRRP work, first create one virtual IP address and MAC address. In this way, add one virtual device in the network. However, when the host in the network communicates with the virtual device, do not need to know any information of the physical device on the network. One virtual device comprises one host (master) and several slave devices (backup). The master device realizes the real forwarding function. When the master device fails, the slave device becomes the new master device and takes over its work.

The master device mentioned in the following text is replaced by “Master” and the slave device is replaced by “Backup”.

NOTE

- VRRP support available in the MTS2800 series, but not in MTS2600 series devices.

67.2 VRRP Function Configuration

Table 67–1 VRRP Function Configuration List

Configuration Task	
Configure the VRRP basic functions	Enable the VRRP protocol
	Configure the VRRP priority
	Configure the VRRP preemption mode
	Configure the real MAC address of VRRP
Configure the VRRP association group	Configure the VRRP association group
Configure the VRRP network authentication	Configure the VRRP simple text authentication

Configuration Task	
Configure VRRP to link with Track	Configure VRRP to link with Track to monitor the Master uplink line
	Configure VRRP to link with Track to monitor the Master and Backup interconnection line

67.2.1 Configure VRRP Basic Functions *-S -E -A*

In the configuration tasks of VRRP, first enable the VRRP protocol and the virtual IP address of the VRRP group needs to be in the same segment as the IP address of the interface so that the configured other functions can take effect.

Configuration Conditions

Before configuring the VRRP basic functions, first complete the following task:

- Configure the IP address of the interface

Enable VRRP Protocol

To enable the VRRP function, you need to create the VRRP group and configure the virtual IP address in the interface.

Table 67–2 Enable the VRRP Protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the VRRP group	**vrrp** *vrid* **ip** *ip-address*	Mandatory Enable the VRRP protocol. VRID is the number of the VRRP group; ip-address is the virtual IP address.

Configure VRRP Priority

After configuring VRRP and if not setting priority, the default priority is 100. The device with high priority is elected as the Master for forwarding the packet and the other become Backup. If the priorities of all devices are equal, elect according to the interface IP address of the device. The one with large interface IP address becomes Master. We can set the VRRP priority as desired. The larger the value is, the higher the priority is.

Table 67–3 Configure the VRRP Priority

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the VRRP group priority	**vrrp** *vrid* **priority** *priority*	Mandatory Configure the VRRP priority; the default priority is 100.

NOTE

- In the virtual MAC mode, when the interface IP address is the same as the virtual IP address, it immediately becomes the Init state and the priority keeps unchanged. If the user needs to configure the virtual IP address the same as the interface IP address, it is necessary to change the virtual MAC mode to the real MAC mode.

Configure VRRP Preemption Mode

After configuring VRRP, in the preemption mode, once other device in the VRRP group discovers that its priority is higher than that of the current Master, it becomes Master; in non-preemption mode, as long as Master does not fail, even the other device has higher priority, it cannot become Master.

Table 67–4 Configure the VRRP Preemption Mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the VRRP group as the preemption mode	**vrrp** *vrid* **preempt**	Mandatory By default, enable the preemption mode

Configure Real MAC Address of VRRP

One virtual device in the VRRP group has one virtual MAC address. According to RFC2338, the format of the virtual MAC address is 00-00-5E-00-01-{vrid}. When the virtual device replies the ARP request, the replied is virtual MAC address, but not the real MAC address of the interface. By default, the used is the virtual MAC address of the interface.

Table 67–5 Configure the Real MAC Address of VRRP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure VRRP to use the real MAC address	**vrrp** *vrid* **use-bia**	Mandatory By default, use the virtual MAC address.

NOTE

- By default, after configuring VRRP, the used is the virtual MAC address. After configuring the command, use the real MAC. That is, when the host sends the packet, forward by the real MAC address; after deleting the command, use the virtual MAC address. That is, when the host sends the packet, use the virtual MAC address to forward.

67.2.2 Configure VRRP Link Group *-S -E -A*

VRRP link group can reduce the interacting of the VRRP packets and the network load, realizing the load balance. Add the common VRRP group to multiple VRRP link groups and the VRRP group plays different roles in different link groups, such as Active or non-Active state. The link group in the Active state is responsible for sending the packet and the non-Active link group serves as standby, so as to reduce the interacting of the packet. Moreover, the link group can configure the sending period of the VRRP packet to ms level, improving the configuration range of the sending period of the general VRRP group packet.

Configuration Conditions

Before configuring the VRRP link group, first complete the following task:

- Configure multiple VRRP groups

Configure VRRP Link Group

Enable the VRRP link group on the sub interface of the VRRP device and the Active group in the link group sends the packet. The non-Active group status and the Active group status keep consistent, that is, when the Active group status switches, the non-Active group status also switches.

Table 67–6 Configure the VRRP Link Group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the link group	**vrrp linkgroup** *lgid* [**interval** *Interval-time*]	Mandatory By default, the Interval-time value is 1000ms
Enter the interface configuration mode	**Interface** *interface-name*	Mandatory
Add the VRRP general group to the link group by the Active mode	**vrrp** *vrid* **linkgroup** lgid [**active**]	Mandatory If not selecting active, add by non-Active mode.

NOTE

- Besides the link group, multiple VRRP groups also can realize the load balance. For details, refer to the chapter of “Configure VRRP Load Balance” in “VRRP Typical Configuration Example”.
- In the link group, after the VRRP general group is added, the general group timer becomes invalid, that is, the sending period of the general group VRRP packets takes the timer of the link group as reference.

67.2.3 Configure VRRP Network Authentication *-S -E -A*

VRRP supports the simple text authentication. The set length of the text authentication cannot 8-bit authentication word.

Configuration Conditions

Before configuring the VRRP network authentication, first complete the following task:

- Configure one VRRP group

Configure VRRP Simple Text Authentication

Table 67–7 Configure the VRRP Simple Text Authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**Interface** *interface-name*	Mandatory
Configure the VRRP simple text authentication	**vrrp** *vrid* **authentication text** *string*	Mandatory By default, do not enable the simple text authentication function. The authentication password can be 8 characters at most.

67.2.4 Configure VRRP to Link with Track *-S -E -A*

VRRP can monitor the status of the uplink line and Master, Backup interconnection line to improve the VRRP reliability.

Configuration Conditions

Before configuring VRRP to link with Track, first complete the following task:

- Configure one VRRP group

Configure VRRP to Link with Track to Monitor Master Uplink Line

On Master, configure linking with Track. It can associate with the interface via Track, or associate with BFD, RTR to make it concern the status of the uplink interface. After the uplink interface is down, VRRP can reduce the Master priority via the configured decrement. Here, after Backup receives, it automatically switches to Master (note that the Master priority is lower than Backup priority). If it is necessary to switch Backup fast, we can configure receiving low-priority fast switching command on Backup. For details, refer to the following figure.

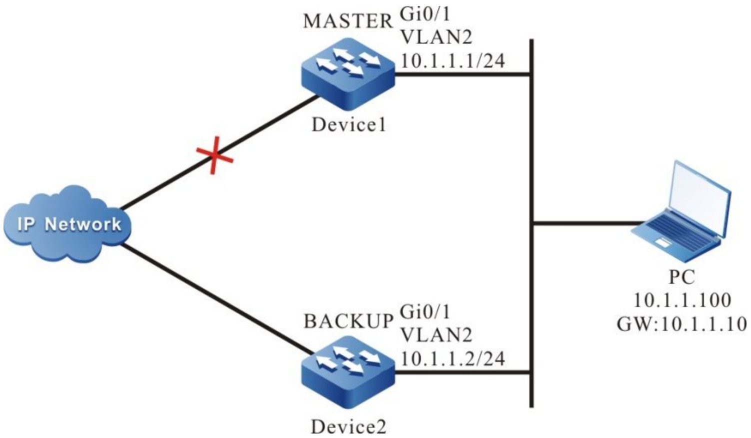


Figure 67–1 Configure VRRP to Link with Track to Monitor Master Uplink Line

Configure VRRP to Link with Track to Associate with Uplink Interface

Associate VRRP with the concerned uplink interface via Track. When the uplink interface is down, Master automatically reduces its own priority. Here, Backup receives the low-priority VRRP packet and switches to Master. If the user is configured with “Receive low-priority packet fast switching”, that is, low-pri-master function, Backup fast switches to Master.

Table 67–8 Configure VRRP to Link with Track to Associate with Uplink Interface (Configure on Master)

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**Interface** *interface-name*	Mandatory
Configure VRRP to associate with the uplink interface	**vrrp** *vrid* **track** *interface-name* [*decrement*]	Mandatory By default, the priority decrement is 10.
Configure VRRP receiving low-priority packet fast switching function	**vrrp** *vrid* **switchover low-pri-master**	Optional The command is configured on Backup to switch fast when the Master priority is reduced.

Configure VRRP to Link with Track (Track Linking with BFD, RTR and so on)

If Track is associated with BFD, RTR and so on, Master can directly associate with Track, so as to monitor the line. When the line fails, Master reduces its own priority. Here, Backup receives the low-priority VRRP packet and switches to Master. If the user is configured with “Receive low-priority packet fast switching”, that is, low-pri-master function, Backup fast switches to Master.

Table 67–9 Configure Master to Link with Track (Track Linking with BFD, RTR and so on)

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**Interface** *interface-name*	Mandatory
Configure VRRP to associate with the uplink interface	**vrrp** *vrid* **track** *track-id* [*decrement*]	Mandatory By default, the priority decrement is 10.
Configure VRRP receiving low-priority packet fast switching function	**vrrp** *vrid* **switchover low-pri-master**	Optional The command is configured on Backup to switch fast when the Master priority is reduced.

NOTE

- For the configuration method of creating Track, Track associating with BFD or RTR, refer to Track configuration manual.
- If the low-pri-master function is configured and when Backup receives the low-priority packet, even it is non-preemption mode, it also switches fast. If the function is not configured when receiving the low-priority packet, Backup switches after the next timeout. If the switching time requirement is not strict, do not need to configure the low-pri-master function, but if the switching time requirement is strict, the function can make the switching time reach the ms level.

Configure VRRP to Associate with Track to Monitor Master and Backup Interconnection Line

Configure VRRP to associate with track to monitor Master and Backup interconnection line. If the line between Master and Backup is down, Backup fast switches to Master. For details, refer to the following figure.

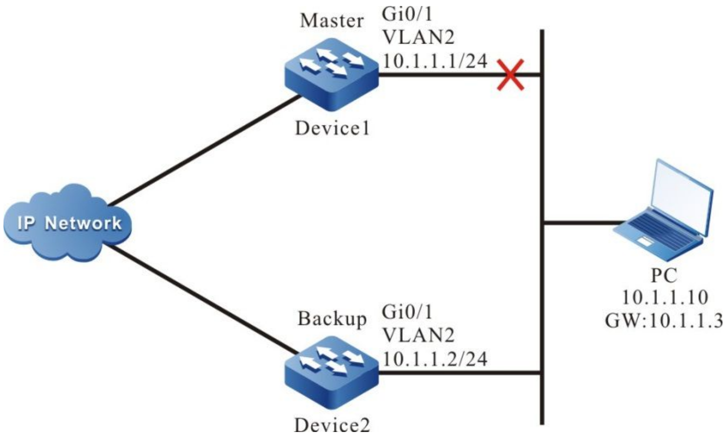


Figure 67–2 Configure VRRP to Associate with Track To Monitor Master and Backup Interconnection Line

Table 67–10 Configure VRRP to Associate with Track to Monitor Master and Backup Interconnection Line

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the fast switching function when Backup VRRP device finds that the line between Master and Backup is down	**vrrp** *vrid* **track** *track-id* **switchover**	Mandatory

NOTE

- For the configuration of Track associating BFD and RTR, refer to Track Configuration Manual.
- Track can associate with BFD to monitor the status of the line between Master and Backup.

67.2.5 VRRP Monitoring and Maintaining *-S -E -A*

Table 67–11 VRRP Monitoring and Maintaining

Command	Description
show vrrp [*brief*] | [**interface** *interface-name*] | [[*linkgroup-number*]] | [*timer*]	Display the VRRP configuration information, including virtual IP address information, virtual MAC address information, device status, device priority, dependent device interface address, link group information and so on.

67.3 VRRP Typical Configuration Example

67.3.1 Configure VRRP Single-backup Group *-S -E -A*

Network Requirements

- On Device1 and Device2, create one single VRRP backup group so that Device1 and Device2 share one virtual IP address, realizing the backup for the default gateway of the user host and reducing the interruption time of the network.

Network Topology

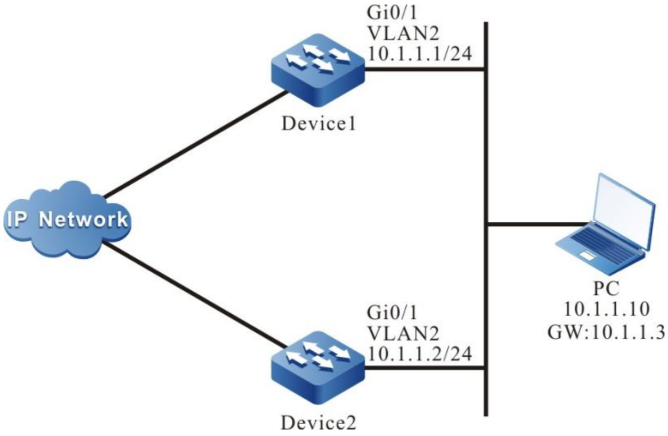


Figure 67–3 Networking of Configuring VRRP Single Backup Group

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN.(Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Create the VRRP group.

#On Device1, configure VRRP group 1, the virtual IP address is 10.1.1.3, and configure the priority as 110.

```
Device1#configure terminal
```

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group1 and the virtual IP address is 10.1.1.3.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

Step 4: Check the result.

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
 Pri-addr : 10.1.1.1
 Vrf : 0
 Virtual router : 1
  Virtual IP address : 10.1.1.3
  Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
  Depend prefix:10.1.1.1/24
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
 Pri-addr : 10.1.1.2
 Vrf : 0
 Virtual router : 1
  Virtual IP address : 10.1.1.3
  Virtual MAC address : 00-00-5e-00-01-01
  Depend prefix:10.1.1.2/24
  State : Backup
  Master addr : 10.1.1.1
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None
```

We can see that the VRRP status of Device1 is Master and the VRRP status of Device2 is Backup. Device1 and Device2 share one virtual IP address. The host communicates with the network via the address. When Device1 fails, Device2 switches to Master at once for forwarding data.

NOTE

- The election principle of the VRRP status is by priority. The one with large priority is Master. If the priorities are the same, compare according to the IP address of the interface. The one with large IP address is Master.
- By default, VRRP works in the preemption mode. The default priority is 100.

67.3.2 Configure VRRP Multi-backup Group *-S -E -A*

Network Requirements

- VRRP multi-backup group is VRRP link group. On Device1 and Device2 interface, enable VRRP and add to the link group. Only the Active group in the link group interacts the protocol packets.
- The VRRP status of the non-Active keeps consistent with the VRRP status of the Active group. When the Active group status switches, the non-Active group also switches.

Network Topology

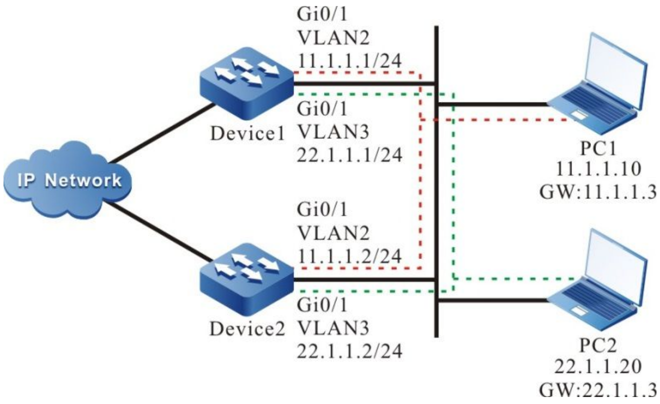


Figure 67–4 VRRP Multi-backup Group Networking

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN.(Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Create one VRRP link group.

#Configure VRRP link group 1 on Device1.

```
Device1#configure terminal
Device1(config)#vrrp linkgroup 1
```

#Configure VRRP link group 1 on Device2.

```
Device2#configure terminal
Device2(config)#vrrp linkgroup 1
```

Step 4: Create the VRRP group.

#Configure the virtual IP address of the VRRP group 1 as 11.1.1.3 on Device1 interface.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 11.1.1.3
Device1(config-if-vlan2)#exit
```

#Configure the virtual IP address of the VRRP group 2 as 22.1.1.3 on Device1 interface.

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#vrrp 2 ip 22.1.1.3
Device1(config-if-vlan3)#exit
```

#Configure the virtual IP address of the VRRP group 1 as 11.1.1.3 on Device2 interface.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 11.1.1.3
Device2(config-if-vlan2)#exit
```

#Configure the virtual IP address of the VRRP group 2 as 22.1.1.3 on Device2 interface.

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#vrrp 2 ip 22.1.1.3
Device2(config-if-vlan3)#exit
```

Step 5: Configure VRRP to add to the link group.

#On Device1, the VRRP group 1 is added to the link group in Active mode.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 linkgroup 1 active
Device1(config-if-vlan2)#exit
```

#On Device1, the VRRP group 2 is added to the link group in non-Active mode.

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#vrrp 2 linkgroup 1
Device1(config-if-vlan3)#exit
```

#On Device2, the VRRP group 1 is added to the link group in Active mode.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 linkgroup 1 active
Device2(config-if-vlan2)#exit
```

#On Device2, the VRRP group 2 is added to the link group in non-Active mode.

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#vrrp 2 linkgroup 1
Device2(config-if-vlan3)#exit
```

Step 6: Check the result.

#View the VRRP status on Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 11.1.1.1
  Vrf : 0
  Virtual router : 1
    Linkgroup : 1
    Active : TRUE
    Virtual IP address : 11.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1.1/24
    State : Backup
    Master addr : 11.1.1.2
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
```

```
Interface vlan3 (Flags 0x1)
 Pri-addr : 22.1.1.1
 Vrf : 0
 Virtual router : 2
  Linkgroup : 1
  Active : FALSE
  Virtual IP address : 22.1.1.3
  Virtual MAC address : 00-00-5e-00-01-02
  Depend prefix:22.1.1.1/24
  State : Backup
  Master addr : 0.0.0.0
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
Authentication Mode : None
```

#View the VRRP status on Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
 Pri-addr : 11.1.1.2
 Vrf : 0
 Virtual router : 1
  Linkgroup : 1
  Active : TRUE
  Virtual IP address : 11.1.1.3
  Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
  Depend prefix:11.1.1.2/24
  State : Master
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None

Interface vlan3 (Flags 0x1)
 Pri-addr : 22.1.1.2
 Vrf : 0
 Virtual router : 2
  Linkgroup : 1
  Active : FALSE
  Virtual IP address : 22.1.1.3
  Virtual MAC address : 00-00-5e-00-01-02 , installed into HW
  Depend prefix:22.1.1.2/24
  State : Master
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
Authentication Mode : None
```

We can see that the VRRP status of the non-Active group and Active group keep consistent.

Step 7: Configure the priority of VLAN2 interface in Device1 as 110, making the status change.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#View the VRRP status on Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
 Pri-addr : 11.1.1.1
```

```
  Vrf : 0
  Virtual router : 1
    Linkgroup : 1
    Active : TRUE
    Virtual IP address : 11.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
    Depend prefix:11.1.1.1/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None

Interface vlan3 (Flags 0x1)
  Pri-addr : 22.1.1.1
  Vrf : 0
  Virtual router : 2
    Linkgroup : 1
    Active : FALSE
    Virtual IP address : 22.1.1.3
    Virtual MAC address : 00-00-5e-00-01-02 , installed into HW
    Depend prefix:22.1.1.1/24
    State : Master
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
```

#View the VRRP status on Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 11.1.1.2
  Vrf : 0
  Virtual router : 1
    Linkgroup : 1
    Active : TRUE
    Virtual IP address : 11.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1.2/24
    State : Backup
    Master addr : 11.1.1.1
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None

Interface vlan3 (Flags 0x1)
  Pri-addr : 22.1.1.2
  Vrf : 0
  Virtual router : 2
    Linkgroup : 1
    Active : FALSE
    Virtual IP address : 22.1.1.3
    Virtual MAC address : 00-00-5e-00-01-02
    Depend prefix:22.1.1.2/24
    State : Backup
    Master addr : 0.0.0.0
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
```

We can see that when the status of the Active group switches, the non-Active group also changes and keeps consistent with the Active group. The Active group in the link group is responsible for sending the protocol packets, but the non-Active group does not send packets. This can reduce the interacting of the protocol packets and the network load.

NOTE

- The sending interval granularity can be smaller. The minimum can be configured to the ms level, so as to reach the 50ms fast switching.

67.3.3 Configure VRRP to Link with Track *-S -E -A*

Network Requirements

- Enable VRRP between Device1 and Device2; Device1 and Device2 share one virtual IP address, realizing the backup of the default gateway of the user host.
- Device1 monitors the status of the interface VLAN3 via Track. When the uplink port VLAN3 of Device1 is down, VRRP can feel and switch the status, making Backup become new Master for forwarding data.

Network Topology

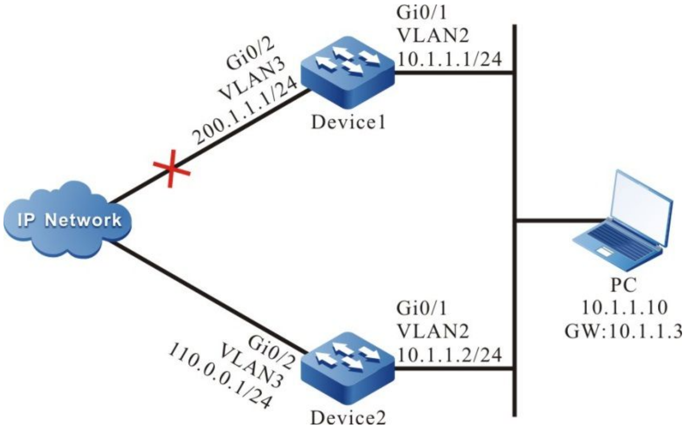


Figure 67–5 Networking of VRRP Linking with Track

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN.(Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Create the VRRP group.

#Configure the VRRP group 1 on Device1; the virtual IP address is 10.1.1.3 and the priority is 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
```

```
Device1(config-if-vlan2)#exit
```

#Configure the VRRP group 1 on Device2; the virtual IP address is 10.1.1.3.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
    Depend prefix:10.1.1.1/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.2
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:10.1.1.2/24
    State : Backup
    Master addr : 10.1.1.1
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
```

Step 4: Configure VRRP to link with Track.

#On Device1, configure VRRP to link with Track and monitor the uplink interface VLAN3; configure the priority decrement as 20.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 track vlan3 20
Device1(config-if-vlan2)#exit
```

# View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
    Depend prefix:10.1.1.1/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
      Track interface : vlan3
      Reduce : 20
      Reduce state : NO
```

When the uplink interface VLAN3 of Device1 is down, the VRRP priority is reduced by 20. Here, the priority of Device2 is high, so the status changes.

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:10.1.1.1/24
    State : Backup
    Master addr : 10.1.1.2
    Normal priority : 110
    Currnet priority : 90
    Priority reduced : 20
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
      Track interface : vlan3
      Reduce : 20
      Reduce state : YES
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.2
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
    Depend prefix:10.1.1.2/24
    State : Master
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
Authentication Mode : None
```

NOTE

- If the association of VRRP and Track needs to reach the fast switching, we can configure switchover low-pri-master on Backup.

67.3.4 Configure VRRP to Link with BFD *-S -E -A*

Network Requirements

- Enable VRRP between Device1 and Device2.

- The VRRP status switching time of Device1 and Device2 needs at least 3s and the service interruption time is long. It is necessary to configure the VRRP and BFD association on Device1 and Device2, realizing the ms-level switching.

Network Topology

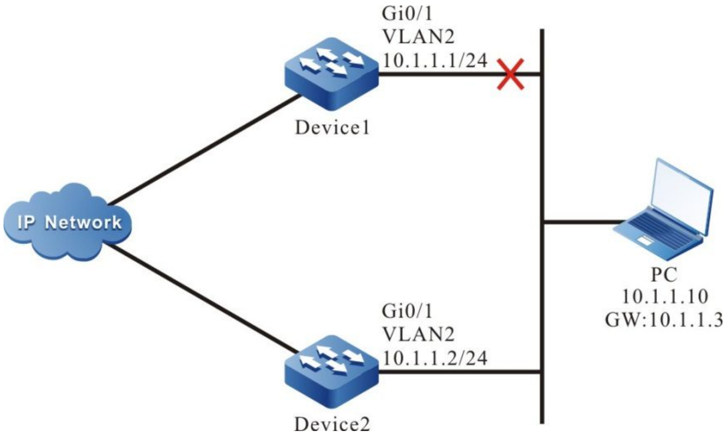


Figure 67–6 Networking of VRRP Linking with BFD

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN.(Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Create the VRRP group.

#Configure the VRRP group 1 on Device1; the virtual IP address is 10.1.1.3 and the priority is 105.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 105
Device1(config-if-vlan2)#exit
```

#Configure the VRRP group 1 on Device2; the virtual IP address is 10.1.1.3.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.2
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
    Depend prefix:10.1.1.2/24
    State : Master
    Normal priority : 105
    Currnet priority : 105
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.2
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:10.1.1.2/24
    State : Backup
    Master addr : 10.1.1.1
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
```

Step 4: Configure Track to link with BFD.

#Configure Track to link with BFD on Device1.

```
Device1(config)#track 1
Device1(config-track)#bfd interface vlan2 remote-ip 10.1.1.2 local-ip 10.1.1.1
Device1(config-track)#exit
```

#Configure Track to link with BFD on Device2.

```
Device2#configure terminal
Device2(config)#track 1
Device2(config-track)#bfd interface vlan2 remote-ip 10.1.1.1 local-ip 10.1.1.2
Device2(config-track)#exit
```

#View the BFD status on Device1.

```
Device1#show bfd session
OurAddr          NeighAddr        LD/RD        State      Holddown      interface
10.1.1.1         10.1.1.2         6/7          UP         5000          vlan2
```

#View the BFD status on Device2.

```
Device2#show bfd session
OurAddr          NeighAddr        LD/RD        State      Holddown      interface
10.1.1.2         10.1.1.1         7/6          UP         5000          vlan2
```

Step 5: Configure VRRP to link with Track.

#Configure VRRP to link with Track on Device2 and configure switchover.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 track 1 switchover
Device2(config-track)#exit
```

Step 6: Check the result.

#View the VRRP status on Device2.

```
Device2#show vrrp
 Interface vlan2 (Flags 0x1)
 Pri-addr : 10.1.1.1
 Vrf : 0
 Virtual router : 1
  Virtual IP address : 10.1.1.3
  Virtual MAC address : 00-00-5e-00-01-01
  Depend prefix:10.1.1.1/24
  State : Backup
  Master addr : 10.1.1.2
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None
   Track object : 1
   Switchover state : NO
```

When Device1 line fails, BFD session is down and Track also becomes down. Device2 feels at once and switches to Master forwarding data.

#View the BFD and VRRP status on Device2.

```
Device2#show bfd session
OurAddr         NeighAddr         LD/RD        State       Holddown     interface
10.1.1.2        10.1.1.1          7/0          DOWN        5000         vlan2
Device2#show vrrp
Interface vlan2 (Flags 0x1)
 Pri-addr : 10.1.1.2
 Vrf : 0
 Virtual router : 1
  Virtual IP address : 10.1.1.3
  Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
  Depend prefix:10.1.1.2/24
  State : Master
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None
   Track object : 1
   Switchover state : YES
```

NOTE

- When VRRP links with Track, Switchover needs to be configured on Backup. Once finding Track down, switch to Master at once.

67.3.5 Configure VRRP Load Balance *-S -E -A*

Network Requirements

- Device1 and Device2 belong to two VRRP groups at the same time; Device1 is Master in group1 and Backup in group2; Device2 is Backup in group1 and Master in group2.
- PC1 forwards data via Device1 and PC2 forwards data via Device2, realizing the load balance.

Network Topology

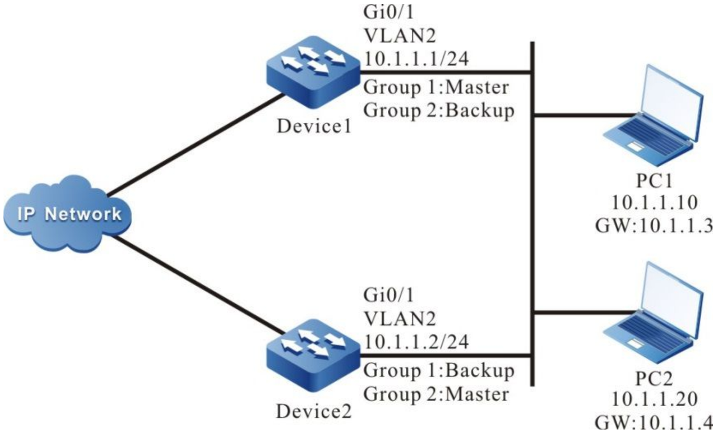


Figure 67–7 VRRP Load Balance Networking

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN.(Omitted)

Step 2: Configure the IP address of the interface.(Omitted)

Step 3: Create the VRRP group 1.

#Configure the VRRP group 1 on Device1; the virtual IP address is 10.1.1.3 and the priority is 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#Configure the VRRP group 1 on Device2; the virtual IP address is 10.1.1.3.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

Step 4: Create VRRP group 2.

#Configure the virtual IP address of VRRP group2 as 10.1.1.4 on Device1.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 2 ip 10.1.1.4
Device1(config-if-vlan2)#exit
```

#Configure the virtual IP address of VRRP group2 as 10.1.1.4 on Device2 and configure the priority as 110.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 2 ip 10.1.1.4
Device2(config-if-vlan2)#vrrp 2 priority 110
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#View the status of VRRP in group1 and group2 on Device1.

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
    Depend prefix:10.1.1.1/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None

  Virtual router : 2
    Virtual IP address : 10.1.1.4
    Virtual MAC address : 00-00-5e-00-01-02
    Depend prefix:10.1.1.1/24
    State : Backup
    Master addr : 10.1.1.2
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
Authentication Mode : None
```

#View the status of VRRP in group1 and group2 on Device2.

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 10.1.1.2
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 10.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:10.1.1.2/24
    State : Backup
    Master addr : 10.1.1.1
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None

  Virtual router : 2
    Virtual IP address : 10.1.1.4
    Virtual MAC address : 00-00-5e-00-01-02 , installed into HW
    Depend prefix:10.1.1.2/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None
```

We can see that Device1 serves as Master of VRRP group1 and Backup of VRRP group2. In contrast with Device1, Device2 serves as Master of VRRP group 2 and Backup of VRRP group 1. When one device fails, two PCs forward data via the other device. This realizes the load balance and backup for each other.

68 VRRPv3

68.1 Overview

VRRPv3 (Virtual Router Redundancy Protocol Version 3) is one fault tolerance protocol. It ensures that when the next-hop device of the host fails, it can be replaced by another device in time, so as to ensure the continuity and reliability of the communication. To make VRRPv3 work, first create one virtual IP address and MAC address. In this way, add one virtual device in the network. However, when the host in the network communicates with the virtual device, do not need to know any information of the physical device on the network. One virtual device comprises one host (master) and several slave devices (backup). The master device realizes the real forwarding function. When the master device fails, the slave device becomes the new master device and takes over its work.

The master device mentioned in the following text is replaced by “Master” and the slave device is replaced by “Backup”.

68.2 VRRPv3 Function Configuration

Table 68–1 VRRPv3 Function Configuration List

Configuration task	
Configure the VRRPv3 basic functions	Configure the VRRPv3 protocol
	Configure the VRRPv3 priority
	Configure the VRRPv3 preemption mode
	Configure the virtual MAC address of VRRPv3
Configure VRRPv3 to link with Track	Configure VRRPv3 to link with Track to monitor the Master uplink line
	Configure VRRPv3 to link with Track to monitor the Master and Backup interconnection line

68.2.1 Configure VRRPv3 Basic Functions *-E -A*

In the configuration tasks of VRRPv3, first enable the VRRPv3 protocol and the virtual IPv6 link-local address of the VRRPv3 group needs to be enabled in the IPv6 link-local address of the interface so that the configured other functions can take effect.

Configuration Conditions

Before configuring the VRRPv3 basic functions, first complete the following task:

- Enable the IPv6 link-local address of the interface.

Configure the VRRPv3 Protocol

To enable VRRPv3 function, it is necessary to create VRRPv3 group under the interface and configure IPv6 link-local virtual address. To configure a global virtual address, the virtual address must have the same network segment as the global real address on the interface.

Table 68–2 Enable the VRRPv3 Protocol

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Required
Configure the link-local virtual address of VRRPv3 group	**ipv6 vrrp** *vrid* **ip** *ip-address* **link-local**	Required By default, do not enable VRRPv3
Configure the global virtual address of VRRPv3 group	**ipv6 vrrp** *vrid* **ip** *ip-address*	Optional The configured global virtual address must be in the same network segment as the global real address on the interface By default, do not enable the global virtual address

Configure the VRRPv3 Priority

After configuring VRRPv3 and if not setting priority, the default priority is 100. The device with high priority is elected as the Master for forwarding the packet and the other become Backup. If the priorities of all devices are equal, elect according to the interface IPv6 link-local address of the device. The one with large interface IPv6 link-local address becomes Master. We can set the VRRPv3 priority as desired. The larger the value is, the higher the priority is.

Table 68–3 Configure the VRRPv3 Priority

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Required
Configure the VRRPv3 group priority	**ipv6 vrrp** *vrid* **priority** *priority*	Required By default, the VRRPv3 default priority is 100

Configure the VRRPv3 Preemption Mode

After configuring VRRPv3, in the preemption mode, once other device in the VRRPv3 group discovers that its priority is higher than that of the current Master, it becomes Master; in non-preemption mode, as long as Master does not fail, even the other device has higher priority, it cannot become Master.

Table 68–4 Configure theVRRPv3 Preemption Mode

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Required
Configure the VRRPv3 group as the preemption mode	**ipv6 vrrp** *vrid* **preempt**	Required By default, enable the preemption function

Configure the Real MAC Address of VRRPv3

One virtual router in the VRRPv3 group has one virtual MAC address. According to RFC5798, the format of the virtual MAC address is 00-00-5E-00-02-{vrid}. By default, the used is the virtual MAC address.

Table 68–5 Configure the Real MAC Address of VRRPv3

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the interface configuration mode	**interface** *interface-name*	Required
Configure VRRPv3 to use the virtual MAC address	**ipv6 vrrp** *vrid* **use-bia**	Required By default, VRRPv3 will use the virtual MAC address

NOTE

- By default, after configuring VRRPv3, the used is the virtual MAC address. After configuring the command, use the real MAC. That is, when the host sends the packet, forward by the real MAC address; after deleting the command, use the virtual MAC address. That is, when the host sends the packet, use the virtual MAC address to forward.

68.2.2 Configure VRRPv3 to Link with Track *-E -A*

VRRPv3 can monitor the status of the uplink line and Master, Backup interconnection line to improve the VRRPv3 reliability.

Configuration Conditions

Before configuring VRRPv3 to link with Track, first complete the following task:

- Configure one VRRPv3 group

Configure VRRPv3 to Link with Track to Monitor the Master Uplink Line

On Master, configure linking with Track. It can associate with the interface via Track, or associate with BFD, RTR to make it concern the status of the uplink interface. After the uplink interface is down, VRRPv3 can reduce the Master priority via the configured decrement. Here, after Backup receives, it automatically switches to Master (note that the Master priority is lower than Backup priority). If it is necessary to switch Backup fast, we can configure receiving low-priority fast switching command on Backup. For details, refer to the following figure.

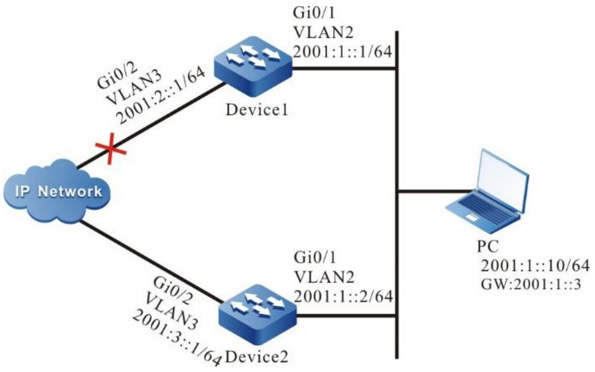


Figure 68-1 Configure VRRPv3 to Link with Track to Monitor Master Uplink Line

Configure VRRPv3 to Link with Track to Associate with Uplink Interface

Associate VRRPv3 with the concerned uplink interface via Track. When the uplink interface is down, Master automatically reduces its own priority. Here, Backup receives the low-priority VRRPv3 packet and switches to Master. If the user is configured with “Receive low-priority packet fast switching”, that is, low-pri-master function, Backup fast switches to Master.

Table 68–6 Configure VRRPv3 to Link with Track to Associate with uplink Interface (Configure on Master)

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Required
Configure VRRPv3 to associate with the uplink interface	**ipv6 vrrp** *vrid* **track** *interface-name* [*decrement*]	Required By default, VRRPv3 is not linked with Track
Configure VRRPv3 receiving low-priority packet fast switching function	**ipv6 vrrp** *vrid* **switchover low-pri-master**	Optional By default, the low-pri-master function is not enabled The command is configured on Backup to switch fast when the Master priority is reduced.

Configure VRRPv3 to Link with Track (Track Linking with BFD, RTR and so on)

If Track is associated with BFD, RTR and so on, Master can directly associate with Track, so as to monitor the line. When the line fails, Master reduces its own priority. Here, Backup receives the low-priority VRRPv3 packet and switches to Master. If the user is configured with “Receive low-priority packet fast switching”, that is, low-pri-master function, Backup fast switches to Master.

Table 68–7 Configure Master to Link with Track (Track Linking with BFD, RTR and so on)

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-

Steps	Command	Description
Enter the interface configuration mode	**interface** *interface-name*	Required
Configure VRRPv3 to associate with the uplink interface	**ipv6 vrrp** *vrid* **track** *track-id* [*decrement*]	Required By default, VRRPv3 is not linked with Track
Configure VRRPv3 receiving low-priority packet fast switching function	**ipv6 vrrp** *vrid* **switchover low-pri-master**	Optional By default, the low-pri-master function is not enabled The command is configured on Backup to switch fast when the Master priority is reduced.

NOTE

- For the configuration method of creating Track, Track associating with BFD or RTR, refer to Track configuration manual.
- If the low-pri-master function is configured and when Backup receives the low-priority packet, even it is non-preemption mode, it also switches fast. If the function is not configured when receiving the low-priority packet, Backup switches after the next timeout. If the switching time requirement is not strict, do not need to configure the low-pri-master function, but if the switching time requirement is strict, the function can make the switching time reach the ms level.

Configure VRRPv3 to Associate with Track to Monitor Master and Backup Interconnection Line

Configure VRRPv3 to associate with track to monitor Master and Backup interconnection line. If the line between Master and Backup is down, Backup fast switches to Master. For details, refer to the following figure.

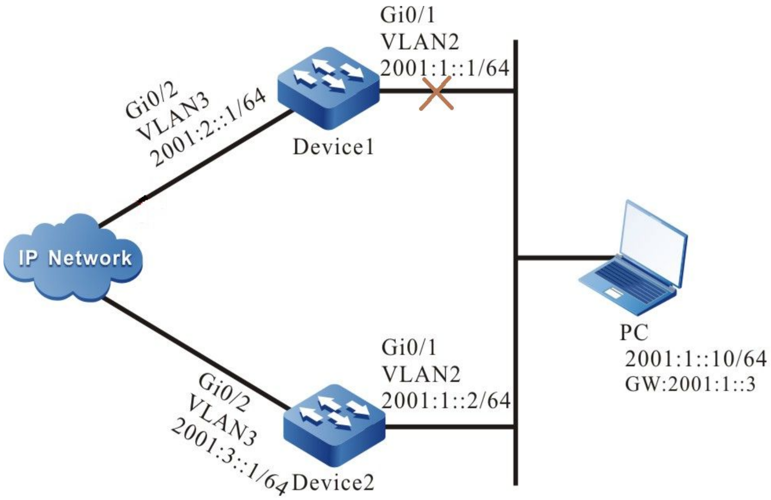


Figure 68-2 Configure VRRPv3 to Associate with Track to Monitor Master and Backup Interconnection Line

Table 68–8 Configure VRRPv3 to Associate with Track to Monitor Master and Backup Interconnection Line

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Required
Configure the fast switching function when Backup VRRPv3 device finds that the line between Master and Backup is down	**ipv6 vrrp** *vrid* **track** *track-id* **switchover**	Required By default, VRRPv3 is not linked with Track

NOTE

- For the configuration of Track associating BFD and RTR, refer to Track Configuration Manual.
- Track can associate with BFD to monitor the status of the line between Master and Backup.

68.2.3 VRRPv3 Monitoring and Maintaining *-E -A*

Table 68–9 VRRPv3 Monitoring and Maintaining

Command	Description
show ipv6 vrrp [**interface** *interface-name*] | [**brief**]	Display the VRRPv3 configuration information, including virtual IP address information, virtual MAC address information, device status, device priority, dependent device interface address and so on.

68.3 VRRPv3 Typical Configuration Example

68.3.1 Configure the Single IPv6 VRRP Backup Group *-E -A*

Network Requirements

- On Device1 and Device2, create the single IPv6 VRRP backup group so that Device1 and Device2 share the same virtual IPv6 link-local address and global address, realizing the backup for the default gateway of the user host and reducing the interruption time of the network.

Network Topology

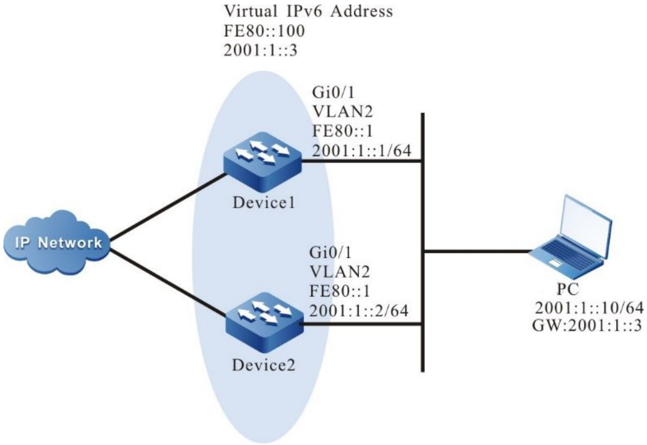


Figure 68-3 Networking of the Single IPv6 VRRP Backup Group

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 address of each interface, and switch on RA response and RA periodic sending.

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
```

```
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
Device2(config-if-vlan2)#no ipv6 nd suppress-ra response
Device2(config-if-vlan2)#exit
```

Step 3: Create the IPv6 VRRP group.

#On Device1, configure VRRP group 1, the virtual IP addresses are 2001:1::3 and fe80::100, and configure the priority as 110.

```
      Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group1 and the virtual IP addresses are 2001:1::3 and fe80::100.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit
```

Step 4: Check the result.

#View the IPv6 VRRP status of Device1.

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
 Pri-addr : fe80::1
 Vrf : 0
 Pri-matchaddr : fe80::1
 Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
    Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
```

```
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None
```

#View the IPv6 VRRP status of Device2.

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
  Pri-addr : fe80::2
  Vrf : 0
  Pri-matchaddr : fe80::2
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
        Global Match address : 2001:1::2
        Global Virtual IP address : 2001:1::3
    Virtual MAC address : 00-00-5e-00-02-01
    State : Backup
    Master addr : fe80::1
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None
```

We can see that the VRRP status of Device1 is Master and the VRRP status of Device2 is Backup. Device1 and Device2 share one virtual IP address. The host communicates with the network via the address. When Device1 fails, Device2 switches to Master at once for forwarding data.

NOTE

- By default, VRRPV3 works in the preemption mode. The default priority is 100.
- The election principle of the VRRPV3 status is by priority. The one with large priority becomes Master preemptively. If the priorities are the same, compare according to the IP link-local address of the interface. The one with large IP address becomes Master preemptively.

68.3.2 Configure IPv6 VRRP to Link with Track *-E -A*

Network Requirements

- On Device1 and Device2, create the single IPv6 VRRP backup group so that Device1 and Device2 share the same virtual IPv6 link-local address and global address, realizing the backup for the default gateway of the user host and reducing the interruption time of the network.
- Device1 monitors the status of the interface VLAN3 via Track. When the uplink port VLAN3 of Device1 is down, VRRP can sense the down event of monitoring interface and reduce its priority, so that Backup becomes a new Master preemptively and continues forwarding data.

Network Topology

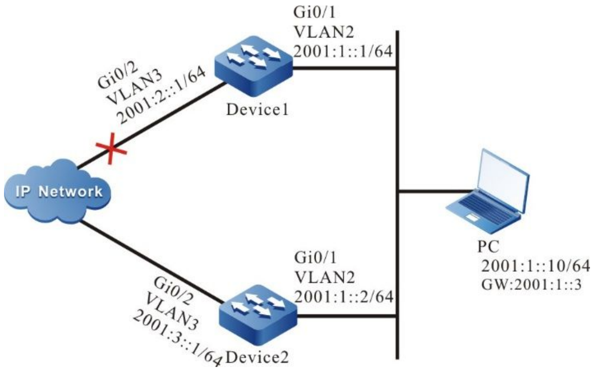


Figure 68-4 Networking of IPv6 VRRP Linking with Track

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 address of each interface, and switch on RA response and RA periodic sending.

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
```

```
Device2(config-if-vlan2)#no ipv6 nd suppress-ra response
Device2(config-if-vlan2)#exit
```

Step 3: Create the IPv6 VRRP group.

#On Device1, configure VRRP group 1, the virtual IP addresses are 2001:1::3 and fe80::100, and configure the priority as 110.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group1 and the virtual IP addresses are 2001:1::3 and fe80::100.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit
```

#View the IPv6 VRRP status of Device1.

```
Device1# show ipv6 vrrp
Interface vlan2 (Flags 0x9)
 Pri-addr : fe80::1
 Vrf : 0
 Pri-matchaddr : fe80::1
 Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
      Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

#View the IPv6 VRRP status of Device2.

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
 Pri-addr : fe80::2
 Vrf : 0
 Pri-matchaddr : fe80::2
 Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::2
      Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Backup
  Master addr : fe80::1
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

Step 4: #Configure VRRP to link with Track.

#Configure VRRPv3 to link with Track on Device1 and monitor the uplink interface VLAN3; configure the priority decrement as 20.

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 track vlan3 20
Device1(config-if-vlan2)#exit
```

#View the IPv6 VRRP status of Device1.

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
 Pri-addr : fe80::1
 Vrf : 0
 Pri-matchaddr : fe80::1
 Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
      Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
   Track interface : vlan3
   Reduce : 20
   Reduce state : NO
```

Step 5: Check the result.

When the monitoring interface VLAN3 of Device1 is down, the VRRP priority is reduced by 20. Here, the priority of Device2 is high, so it becomes Master preemptively with the status change.

#View the IPv6 VRRP status of Device1.

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
 Pri-addr : fe80::1
 Vrf : 0
 Pri-matchaddr : fe80::1
 Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
      Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Backup
  Master addr : fe80::2
  Normal priority : 110
  Currnet priority : 90
  Priority reduced : 20
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
   Track interface : vlan3
   Reduce : 20
   Reduce state : YES
```

#View the IPv6 VRRP status of Device2.

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
 Pri-addr : fe80::2
```

```
Vrf : 0
Pri-matchaddr : fe80::2
Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
      Global Match address : 2001:1::2
          Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Master
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

68.3.3 Configure the Load Balance of IPv6 VRRP *-E -A*

Network Requirements

- On Device1 and Device2, create two IPv6 VRRP backup groups. Device1 and Device2 belong to two VRRP groups at the same time; Device1 is Master in group1 and Backup in group2; Device2 is Backup in group1 and Master in group2.
- PC1 forwards data via Device1 and PC2 forwards data via Device2, realizing the load balance.

Network Topology

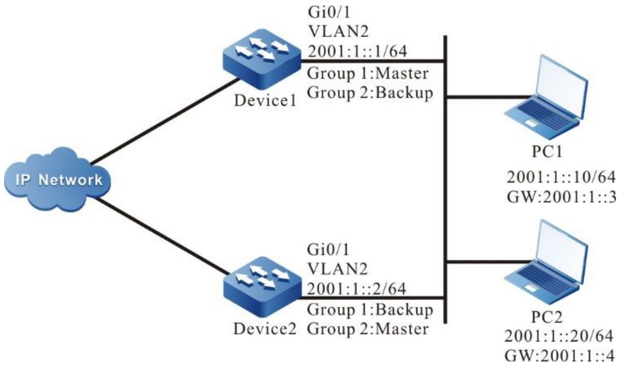


Figure 68-5 Configure IPv6 VRRP Load Balance Networking

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IPv6 address of each interface, and switch on RA response and RA periodic sending.

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
Device2(config-if-vlan2)#no ipv6 nd suppress-ra respons
Device2(config-if-vlan2)#exit
```

Step 3: Create the IPv6 VRRP group1.

#On Device1, configure VRRP group 1, the virtual IP addresses are 2001:1::3 and fe80::100, and configure the priority as 110.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group1 and the virtual IP addresses are 2001:1::3 and fe80::100.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit
```

Step 4: Create the IPv6 VRRP group2.

#On Device1, configure VRRP group2 and the virtual IP addresses are 2001:1::4 and fe80::200.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 2 ip fe80::200 link-local
Device1(config-if-vlan2)#ipv6 vrrp 2 ip 2001:1::4
Device1(config-if-vlan2)#exit
```

#On Device2, configure VRRP group2, the virtual IP addresses are 2001:1::4 and fe80::200, and configure the priority as 110.

```
Device2(config)#interface vlan2
```

```
Device2(config-if-vlan2)#ipv6 vrrp 2 ip fe80::200 link-local
Device2(config-if-vlan2)#ipv6 vrrp 2 ip 2001:1::4
Device2(config-if-vlan2)#ipv6 vrrp 2 priority 110
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#On Device1, check the status of IPv6 VRRP in group1 and group2 respectively.

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
 Pri-addr : fe80::1
 Vrf : 0
 Pri-matchaddr : fe80::1
 Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
      Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None

 Pri-matchaddr : fe80::1
 Virtual router : 2
  Mac mode: real mac mode
  Virtual IP address : fe80::200
  Global address count:1
    Global Match address : 2001:1::1
      Global Virtual IP address : 2001:1::4
  Virtual MAC address : 00-00-5e-00-02-02
  State : Backup
  Master addr : fe80::2
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

#On Device2, check the status of IPv6 VRRP in group1 and group2 respectively.

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
 Pri-addr : fe80::2
 Vrf : 0
 Pri-matchaddr : fe80::2
 Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::2
      Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Backup
  Master addr : fe80::1
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None

 Pri-matchaddr : fe80::2
 Virtual router : 2
  Mac mode: real mac mode
  Virtual IP address : fe80::200
  Global address count:1
    Global Match address : 2001:1::2
      Global Virtual IP address : 2001:1::4
  Virtual MAC address : 00-00-5e-00-02-02
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

We can see that Device1 serves as Master of VRRP group1 and Backup of VRRP group2, while Device2 serves as Master of VRRP group2 and Backup of VRRP group1. When one device fails, two PCs forward data via the other device. This realizes the load balance and backup for each other.

69 Track

69.1 Overview

Track can be used to monitor some information when the system runs. The other service modules can be associated with Track so that the service module can monitor the change when the system runs. After the service module is associated with Track and when the information monitored by Track changes, Track informs the service module so that the service module can process correspondingly. For example, in the actual application, VRRP and VBRP often monitor the uplink interface status and network availability by associating with Track and adjust its own priority according to the information, so as to realize the active/standby switchover.

69.2 Track Function Configuration

Table 69–1 Track Function Configuration List

Configuration Task	
Configure the Track group	Configure the Track group
Configure the monitor object	Configure the monitor interface status
	Configure monitoring the status of the switching port
	Configure monitoring the direct route of the interface
	Configure monitoring route reachable
	Configure monitoring the RTR group
	Configure monitoring the BFD session

69.2.1 Configure Track Group *-B -S -E -A*

Configuration Conditions

None

Configure Track Group

The system can configure multiple Track groups. Each Track group is independent from each other. One Track group can include multiple monitor objects.

The Track group has two logics, that is, “and”, “or”:

- When the Track group logic is “and”, all monitor objects in Track group need to be up so that the Track group can be up; on contrast, it is down.
- When the Track group logic is “or”, as long as one monitor object in Track group is up, the Track object status can be up; on contrast, it is down.

Table 69–2 Configure the Track Group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the Track group	**track** *group-id*	Mandatory
Configure Track group logic	**logic operator** { **AND** | **OR** }	Optional **AND**: logic “and” **OR**: logic “or” By default, Track group logic is “or”.

NOTE

- When the service module needs to monitor some information via Track, besides configuring the monitor object in the Track group, we also need to refer to the service module configuration manual and configure the service module to associate with Track group.

69.2.2 Configure Monitor Object -B -S -E -A

Configuration Conditions

Before configuring the monitor object, first complete the following task:

- Configure the Track group

Configure Monitoring Interface Status

We can configure the monitor object as the interface status in the Track group. When the interface network layer protocol is up, the monitor object status is up; when the interface network layer protocol is down, the monitor object status is down.

Table 69–3 Configure Monitoring Interface Status

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	Mandatory
Configure monitoring interface status	**interface** *interface-name* **line-protocol**	Mandatory

Configure Monitoring Switching Port Status

We can configure the monitor object as the status of the switching port in the Track group. When the switching port is up, the monitor object status is up; when the switching port is down, the monitor object status is down.

Table 69–4 Configure Monitoring the Switching Port Status

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	Mandatory
Configure monitoring the status of the switching port	**switchport interface** *interface-name*	Mandatory

Configure Monitoring Direct Route of Interface

We can configure the monitor object as the direct route of the interface in the Track group. When the interface has IP address and the status is up, the status of the monitor object is up; when the interface does not have IP address or the status is down, the status of the monitor object is down.

Table 69–5 Configure Monitoring the Direct Route of the Interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	Mandatory

Step	Command	Description
Configure monitoring the direct route of the interface	**interface** *interface-name* **ip-routing**	Mandatory

Configure Monitoring Route Reachable

We can configure the monitor object as the route reachable in the Track group. When there is the route of the configured network, the status of the monitor object is up; when there is no route of the configured network, the status of the monitor object is down.

Table 69–6 Configure Monitoring Route Reachable

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	Mandatory
Configure monitoring route reachable	**ip-route** *network mask* [**vrf** *vrf-name*] [**metric** *metric-value*]	Mandatory When there is the option **metric**, the route metric to the network needs to be smaller than the configured value so that the status of the monitor object can be up.

Configure Monitoring RTR Group

We can configure the monitor object as the RTR group in the Track group. When the status of the RTR group is reachable, the status of the monitor object is up; when the status of the RTR group is unreachable, the status of the monitor object is down. RTR (Response Time Reporter) is one tool of detecting and monitoring the network. Track can monitor the RTR group to monitor the network communication.

Table 69–7 Configure Monitoring the RTR Group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	Mandatory

Step	Command	Description
Configure monitoring the RTR group	**rtr** *rtr-group-id*	Mandatory

NOTE

- For the configuration of the RTR group, refer to SLA Configuration Manual.

Configure Monitoring BFD Session

We can configure the monitor object as the BFD session in the Track group. When the status of the BFD session is up, the status of the monitor object is up; when the status of the BFD session is down, the status of the monitor object is down. The BFD protocol is one set of standard unified detection mechanism, used to fast detect, monitor the path in the network or the connection status of the IP route forwarding. The network connection status can be monitored indirectly by monitoring the BFD session.

Table 69-8 Configure Monitoring the BFD Session

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	Mandatory
Configure monitoring the BFD session	**bfd interface** *interface-name* **remote-ip** *ip-address* **local-ip** *ip-address*	Mandatory When configuring monitoring the BFD session, it needs to be configured at the two sides of the BFD session. Otherwise, the BFD session cannot be set up successfully.

Table 69–9 Track Monitoring and Maintaining

Command	Description
show track object *group-id*	Display the Track group information.
show track bfd-session	Display the BFD session information monitored by Track.

69.2.3 Track Monitoring and Maintaining *-B -S -E -A*

Table 6–10 Track Monitoring and Maintaining

Command	Description
show track object *group-id*	Display the Track group information.
show track bfd-session	Display the BFD session information monitored by Track.

70 BFD

70.1 Overview

The BFD (Bidirectional Forwarding Detection) protocol is one set of standard unified detection mechanism, used to fast detect, monitor the path in the network or the connection status of the IP route forwarding. It provides a general, standardized, media independent, and protocol independent fast fault detection mechanism, able to quickly detect the line fault between two devices for each upper application (such as routing protocol).

BFD can provide fault detection on any type of path between systems, and the BFD session is established based on the needs of upper applications. If multiple application protocols correspond to the same path, one BFD session can be used for detection.

The processing flow of BFD protocol and upper application protocol includes:

(1) The upper application protocol sends the neighbor information (including the peer IP address, the home IP address, interface) to the BFD protocol.

(2) The BFD protocol queries whether there is a corresponding session. If there is none, it will create the corresponding session according to the received neighbor information, and then the BFD session will send BFD control packets to drive the operation of BFD state machine. The BFD control packet completes the corresponding session through three handshakes. After the transition from the Down (start) state to the Init (initialization) state, and the Init state to the Up (end) state, the session establishment process will negotiate the parameters of the session, including packet sending interval, detection interval and so on.

(3) At the end of the session establishment, the path status is detected by sending detection packets periodically. If no BFD control packet sent by the peer device is received within the detection interval, the BFD protocol will regard that there is a fault in this path and send the fault information to the upper application protocol.

(4) After receiving the fault report, the upper application protocol notifies the BFD protocol to delete the session when enabling or deleting neighbor. If there is no other upper protocol to detect the session link, delete the corresponding session.

In terms of detection path types, there is single hop IP path detection with the home adjacent to the peer and multi hop IP path detection with the home adjacent to the peer. At present, the link of OSPF, RIP, EBGP, ISIS, LDP, RSVP-TE, TRACK and static routing protocols with BFD belongs to single hop IP path detection, while that of IBGP with BFD belongs to multi hop IP path detection.

70.2 BFD Functional Configuration

Table 70–1 BFD Function Configuration List

Configuration task	
Configure BFD Basic Functions	Configure the minimum sending time interval of BFD control packets
	Configure the minimum receiving time interval of BFD control packets
	Configure the detection timeout multiple for the BFD session

70.2.1 Configure BFD Basic Functions *-E -A*

Configuration Conditions

Before configuring the BFD basic functions, first complete the following task:

- The IP address of the interface is configured to make the adjacent node network layers accessible.
- Configure the upper application to be linked with BFD.

Configure the Minimum Sending Time Interval of BFD Control Packets

Table 70–2 Configure the Minimum Sending Time Interval of BFD Control Packets

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the minimum sending time interval of BFD control packets	**bfd min-transmit-interval** *value*	Optional By default, the minimum sending time interval of BFD control packets is 1000ms.

NOTE

- Actual sending time interval of home BFD control packets = MAX (the minimum sending time interval of home BFD control packets and the minimum receiving time interval of peer BFD control packets).
- In the interface mode, the minimum sending time interval of BFD control packets is only valid for single hop IP session.

Configure the Minimum Receiving Time Interval of BFD Control Packets

Table 70–3 Configure the Minimum Receiving Time Interval of BFD Control Packets

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the minimum receiving time interval of BFD control packets	**bfd min-receive-interval** *value*	Optional By default, the minimum receiving time interval of BFD control packets is 1000ms.

NOTE

- Actual sending time interval of peer BFD control packets = MAX (the minimum sending time interval of peer BFD control packets and the minimum receiving time interval of home BFD control packets).
- In the interface mode, the minimum receiving time interval of BFD control packets is only valid for single hop IP session.

Configure the Detection Timeout Multiple for the BFD Session

Table 70–4 Configure the Detection Timeout Multiple for the BFD Session

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-

Steps	Command	Description
Configure the detection timeout multiple for the BFD session	**bfd multiplier** *value*	Optional By default, the detection timeout multiple for the BFD session is 5

NOTE

- To ensure the validity of BFD session detection, be careful to configure the minimum value of the BFD detection timeout multiple.
- Actual detection time of home BFD = detection timeout multiple of peer BFD session × actual sending time interval of peer BFD control packets.
- In the interface mode, the detection timeout multiple of BFD control packets is only valid for single hop IP session.

Configure the Fast Detection Function of BFD Session

Table 70–5 Configure the Fast Detection Function of BFD Session

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the fast detection function of BFD session	**bfd fast-detect**	Optional By default, the fast detection function of BFD session is disabled.

70.2.2 BFD Monitoring and Maintaining *-E -A*

Table 70–6 BFD Monitoring and Maintaining

Command	Description
clear bfd drop statistics	Clear error packet statistics of BFD
clear bfd error-statistics	Clear error statistics of BFD

Command	Description
show bfd	Displays BFD parameters supported by the device
show bfd client [*client-name*]	Display BFD client information
show bfd discriminator	Display BFD identification information
show bfd drop statistics	Display error packet statistics of BFD
show bfd error-statistics	Display error statistics of BFD
show bfd session [*neighbor-ipv4-address*] [**detail**]	Display BFD IPv4 session information
show bfd session ipv6 [*neighbor-ipv6-address* [*interface-name*]] [**detail**]	Display BFD IPv6 session information

70.3 BFD Typical Configuration Example

70.3.1 Configure BFD Basic Functions *-E -A*

Network Requirements

- Device 4 is a connecting device and only supports transparent data transmission.
- Device1, Device2 and Device3 work based on OSPF protocol. Device1 and Device3 are configured with BFD function.
- Modify the BFD parameters, so that when the line between Device4 and Devcie3 fails, the service data between Device1 and Device3 can realize the ms-level switching.

Network Topology

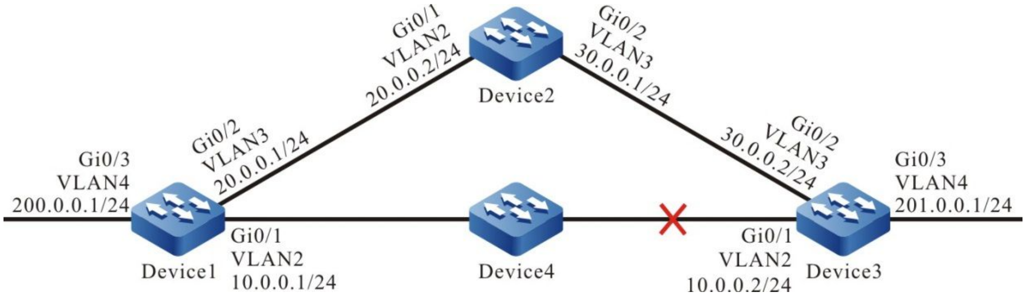


Figure 70-1 Networking of Configuring the BFD Basic Function

Configuration Steps

Step 1: Configure VLAN, and add the port to corresponding VLAN. (omitted)

Step 2: Configure IP address for the ports. (omitted)

Step 3: Configure OSPF.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

Step 4: Configure OSPF to coordinate with BFD.

#Configure Device1.

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf bfd
Device1(config-if-vlan2)#exit
```

#Configure Device3.

```
Device3(config)#bfd fast-detect
Device3(config)#interface vlan2
```

```
Device3(config-if-vlan2)#ip ospf bfd
Device3(config-if-vlan2)#exit
```

#Query the BFD session of Device1.

```
Device1#show bfd session detail
Total session number: 1
OurAddr          NeighAddr          LD/RD          State        Holddown      interface
10.0.0.1         10.0.0.2           12/19          UP           5000          vlan2
Type:direct
Local State:UP  Remote State:UP  Up for: 0h:10m:57s  Number of times UP:1
Send Interval:1000ms  Detection time:5000ms(1000ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:1000  MinRxInt:1000  Multiplier:5
Remote MinTxInt:1000  Remote MinRxInt:1000  Remote Multiplier:5
Registered protocols:OSPF
```

We can see that OSPF and BFD are linked successfully to establish the session is normally, and the detection timeout is 5 seconds.

#Query the routing table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
Gateway of last resort is not set
C   10.0.0.0/24 is directly connected, 00:20:01, vlan2
C   20.0.0.0/24 is directly connected, 00:25:22, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 00:12:31, vlan3
            [110/2] via 10.0.0.2, 00:11:20, vlan2
C   127.0.0.0/8 is directly connected, 00:31:09, lo0
C   200.0.0.0/24 is directly connected, 00:20:10, vlan4
O   201.0.0.0/24 [110/2] via 10.0.0.2, 00:11:30, vlan2
```

It can be seen from the routing table that route 201.0.0.0/24 gives preference to the line between Device1 and Device3 for communication.

Step 5:   Configure the BFD parameters.

#Configure Device1, modify the minimum sending time interval and minimum receiving time interval of BFD control packets to 100ms, and the detection timeout multiple to 3.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#bfd min-transmit-interval 100
Device1(config-if-vlan2)#bfd min-receive-interval 100
Device1(config-if-vlan2)#bfd multiplier 3
Device1(config-if-vlan2)#exit
```

#Configure Device3, modify the minimum sending time interval and minimum receiving time interval of BFD control packets to 100ms, and the detection timeout multiple to 3.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#bfd min-transmit-interval 100
Device3(config-if-vlan2)#bfd min-receive-interval 100
Device3(config-if-vlan2)#bfd multiplier 3
```

Device3(config-if-vlan2)#exit

Step 6: Check the result.

#Query the BFD session of Device1.

```
Device1#show bfd session detail
Total session number: 1
OurAddr          NeighAddr        LD/RD        State      Holddown     interface
10.0.0.1         10.0.0.2         12/19        UP         300          vlan2
Type:direct
Local State:UP  Remote State:UP  Up for: 0h:11m:27s  Number of times UP:1
Send Interval:100ms  Detection time:300ms(100ms*3)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:100  MinRxInt:100  Multiplier:3
Remote MinTxInt:100  Remote MinRxInt:100  Remote Multiplier:3
Registered protocols:OSPF
```

After modifying the BFD parameters, the BFD detection timeout is negotiated from the previous 5 seconds to 300ms.

#When the line between Device1 and Device3 fails, BFD will quickly detect the failure and notify OSPF. OSPF will switch the route to Device2 for communication and view the route table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
Gateway of last resort is not set
C   10.0.0.0/24 is directly connected, 00:25:00, vlan2
C   20.0.0.0/24 is directly connected, 00:30:33, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 00:17:32, vlan3
C   127.0.0.0/8 is directly connected, 00:36:10, lo0
C   200.0.0.0/24 is directly connected, 00:25:11, vlan4
O   201.0.0.0/24 [110/3] via 20.0.0.2, 00:00:10, vlan3
```

By comparing the routing table in step 3, we can see that route 201.0.0.0/24 has been switched to Device2 for communication.

BFD processing on Device3 is similar to that on Device1.

71 ERPS

71.1 Overview

In the Ethernet two-layer network, STP (Spanning Tree Protocol) is generally used for network reliability, but STP (Spanning Tree Protocol) has a convergence time of seconds in general, which is longer when the network diameter is larger. To shorten the convergence time and eliminate the impact of the network size, ERPS (Ethernet Ring Protection Switching) technology came into being. ERPS (Ethernet ring protection switching) is a two-layer ring breaking protocol standard defined by ITU-T and the standard number is ITU-T G.8032/Y1344, also known as G.8032. G.8032 is an Ethernet link layer technology with high reliability and stability. When the Ethernet ring network is intact, it can prevent the hard broadcast dispute of the data ring, and when the Ethernet ring network link fails, it can quickly restore the communication path between nodes in the ring network, with a high convergence rate. Moreover, it will achieve interoperability if the manufacturer's device in the ring network supports this protocol.

ERPS related concepts and definitions:

- ERPS (Ethernet Ring Protection Switching) ring: ERPS ring is a basic unit of ERPS protocol, composed of a group of interconnected network devices configured with the same VLAN. ERPS ring consists of the primary ring and the sub-ring. The primary ring is closed while the sub-ring is non-closed. The properties of the primary ring and the sub-ring are determined by the user.
- Port role: there are three types of port roles specified in ERPS protocol: RPL owner ports, RPL neighbor ports and normal ports. RPL neighbor ports are only supported by ERPSv2 version.
- RPL owner port: an ERPS ring has only one RPL owner port, specified by user configuration. The ERPS protocol blocks the forwarding state of the RPL owner port to prevent the link from looping. The link where the RPL owner port is located is the RPL (Ring Protection Link).
- RPL neighbor port: RPL neighbor port refers to the node port directly connected to the RPL owner port. Under normal circumstances, both the RPL owner port and the RPL neighbor port will be blocked to prevent looping. When the ERPS ring network fails, both the RPL owner port and the RPL neighbor port will be released.
- Regular port: in the ERPS ring, ports other than the RPL owner port and the RPL neighbor port are normal ones. The normal port is responsible for monitoring its own direct link state and informing other node ports of the link state changes in a timely manner.
- ERPS control VLAN: used to transmit ERPS protocol packets. The control VLAN is specified by the user, and the VLAN used as ERPS control VLAN cannot be used for other businesses. The different ERPS ring has a different control VLAN.
- ERPS data instance: data instance that needs VLAN mapping of data protected by ERPS ring.

71.2 ERPS Functional Configuration

Table 71–1 ERPS Function Configuration List

Configuration task	
Configure the ERPS ring	Configure the ERPS ring
	Configure the ERPS protocol
Configure the ERPS ring timer	Configure the ERPS ring timer
Configure ERPS network optimization	Configure the ERPS port blocking switch mode
	Clear ERPS configuration blocking points
	Configure ERPS topology change notifications
	Configure ERPS TC restriction functions
Configure ERPS to link with CFM	Configure ERPS linking with CFM

71.2.1 Configure the ERPS Ring *-B -S -E -A*

When configuring the ERPS ring, the necessary configuration is required for the ports connected to the ERPS ring on all nodes and all nodes on the ring.

Configuration Conditions

Before configuring ERPS, first complete the following task:

- Create a control VLAN;
- Disable the ring network protocol on the ring port;
- Configure the ring port to trunk mode;
- Add the ring port to the control VLAN of the ring;
- Configure the mapping relationship between MSTP instance and VLAN to be included.

Configure the ERPS Ring

Configure the ERPS ring basic functions

Table 71-2 Configure the ERPS Ring

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create the ERPS ring	**erps ring** *ring-id*	Required By default, the ERPS ring is not created, and the ring value range is 1~64
Configure the ERPS ring control VLAN	**control vlan** *vlan-id*	Required By default, the ERPS ring control VLAN is not configured
Configure the ERPS ring data instance	**instance** *instance-list*	Required By default, the ERPS ring data instance is not configured
Configure the ERPS ring port PORT0	**port0** { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* } [**rpl** { **owner** | **neighbour** }]	Required By default, ERPS port0 is not configured **rpl owner**: indicating the port is the owner port of RPL **rpl neighbour:** indicating the port is the neighbor port of RPL No configuration of RPL indicates that the port is a normal port
Configure the ERPS ring port PORT1	**port1** { **interface** *interface-name* | **link-aggregation** *link-*	Required

	aggregation-id } [**rpl** { **owner** | **neighbour** }]	By default, ERPS port1 is not configured **rpl owner**: indicating the port is the owner port of RPL **rpl neighbour:** indicating the port is the neighbor port of RPL No configuration of RPL indicates that the port is a normal port
Configure the ERPS ring version information	**version** { *v1* | *v2* }	Optional V2 by default
Configure the mel value of ERPS ring packets	**mel** *level-id*	Optional By default, the mel value is 7 and the value range is 0~7
Configure the ERPS ring to a sub-ring	**sub-ring**	Optional By default, the ERPS ring is a primary ring
Configure the ERPS ring non cutting-back mode	**revertive disable**	Optional By default, ERPS works in the switching-back mode
Configure the ERPS sub-ring virtual channel	**virtual-channel enable**	Optional By default, ERPS is a non virtual channel

NOTE

- ERPS control VLAN can only be used for ERPS protocol packet transmission, not for other services. All nodes in the same ERPS ring need to be configured with the same mel value

- Use of sub-ring virtual channel for networking in the intersecting ring networking environment is not recommended.

Configure the ERPS Protocol

At the end of the above configuration, use this command to start the ERPS protocol.

Table 71-3 Enable Protocol on the ERPS Ring

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter ERPS configuration mode	**erps ring** *ring-id*	-
Configure the ERPS protocol	**erps enable**	Required By default, the ring does not enable ERPS protocol

71.2.2 Configure the ERPS Ring Timer *-B -S -E -A*

Configuration Conditions

Before configuring ERPS timer, first complete the following task:

- Configure the ERPS ring.

Configure the ERPS Ring Timer

After failure recovery of the node device or link in the ERPS ring, to prevent network oscillations, the timer in the ERPS ring will be enabled to reduce the interruption time of traffic.

Table 71-4 Configure the ERPS Ring Timer

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter ERPS configuration mode	**erps ring** *ring-id*	-
Configure the ERPS ring guard timer	**guard-timer** *time-value*	Required By default, the timeout of Guard timer is 500ms, and

		the range of guard timer is 10~2000ms.
Configure the ERPS ring Hold-off timer	**holdoff-timer** *time-value*	Required By default, the timeout of hold-off timer is 0ms, and the range of hold-off timer is 0~10000ms.
Configure the ERPS ring WTR timer	**wtr-timer** *time-value*	Required By default, the timeout of WTR timer is 5min, and the range of WTR timer is 1~12ms.

71.2.3 Configure ERPS Network Optimization *-B -S -E -A*

Configuration Conditions

Before configuring ERPS network optimization, first complete the following task:

- Configure the ERPS ring.

Configure the ERPS Port Blocking Switch Mode

Because the bandwidth of the link where the RPL owner port is located may carry more user traffic, at this time, blocking the link with low bandwidth can be considered to move the user traffic to the RPL for transmission.

Table 71-5 Configure the ERPS Port Blocking Switch Mode

Steps	Command	Description
Configure the ERPS port blocking switch mode	**erps ring** *ring-id* { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* } **switch** { **force | manual** }	Required By default, the ERPS ring control blocking point switching mode is not configured

Clear ERPS Configuration Blocking Points

Clear ERPS ring configuration blocking point switching operation

Table 71-6 Clear ERPS Configuration Blocking Points

Steps	Command	Description

Clear ERPS configuration blocking points	**clear erps ring** *ring-id*	Required

Configure ERPS Topology Change Notifications

When the topology of the ERPS ring changes and the upper layer 2 network is not informed in time, the MAC address table of the upper layer 2 network will still retain the MAC address table existing before the lower network topology changes, thus leading to the user traffic interruption. To ensure the normal communication of user traffic, it is necessary to select the notification object of topology change of this ERPS ring according to the actual network of users.

Table 71-7 Configure ERPS Ring Topology Change Notifications

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter ERPS configuration mode	**erps ring** *ring-id*	-
Configure ERPS ring topology change notifications	**tc-notify erps ring** *ring-list*	Required By default, the ERPS topology change is not informed.

Configure ERPS TC Restriction Functions

As frequent topology change notification leads to the degradation of CPU processing capacity, and frequent refresh of Flush-FDB packets on the ERPS ring takes up network bandwidth, it is necessary to suppress topology change notification packets in order to prevent them from happening. By configuring the time interval of ERPS topology change protection and the maximum threshold of handling topology change packets within the time interval of topology change protection, the topology change notification can be suppressed and frequent deletion of MAC address table and ARP table can be prevented to protect the device.

Table 71-8 Configure ERPS TC Restriction Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter ERPS configuration mode	**erps ring** *ring-id*	-

Configure ERPS topology change TC restriction function	**tc-limit enable**	Required By default, the TC restriction function is not enabled.
Configure the time interval of TC limit for ERPS topology change	**tc-limit interval** *interval-value*	Optional By default, the time interval is 2 seconds, and the value range is 1~500 seconds.
Configure the threshold for ERPS topology change TC restriction function	**tc-limit threshold** *threshold-value*	Optional By default, the value is 3, and the value range is 1~64.

71.2.4 Configure ERPS to Link with CFM *-B -S -E -A*

Configuration Conditions

Before configuring ERPS to link with CFM (Connectivity Fault Management), first complete the following task:

- Configure the ERPS basic functions.
- Configure the CFM functions.

Configure ERPS to link with CFM

When the Ethernet CFM linkage function is configured on the ring port with ERPS ring, the fault detection can be accelerated to achieve fast convergence of topology and reduce traffic interruption time.

Table 71-9 Configure ERPS to Link with CFM

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2 ethernet interface configuration mode	**interface** *interface-name*	Must be chosen alternatively After entering L2 ethernet interface configuration mode, subsequent configurations only
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

		apply to current port; in aggregation group configuration mode, subsequent configurations only take effect in aggregation group
Configure ERPS to link with CFM	**erps ring** *ring-id* **track cfm md** *md-name* **ma** *ma-name* **mep** *mep-id* **remote-mep** *rmep-id*	Required By default, the port is not linked with CFM.

71.2.5 ERPS Monitoring and Maintaining *-B -S -E -A*

Table 71-10 ERPS Monitoring and Maintaining

Command	Description
clear erps [**ring** *ring-id*] **statistics**	Clear ERPS related statistics
show erps [**ring** *ring-id*] **config**	Display the configuration information of ERPS
show erps [ring *ring-id***] detail**	Display the details of ERPS
show erps [**ring** *ring-id*] **statistics**	Display statistics for ERPS

71.3 ERPS Typical Configuration Example

71.3.1 Configure the ERPS Basic Functions *-B -S -E -A*

Network Requirements

- All devices are in the same layer 2 network.
- Enable ERPS for all devices and break the link in the network through ERPS.

Network Topology

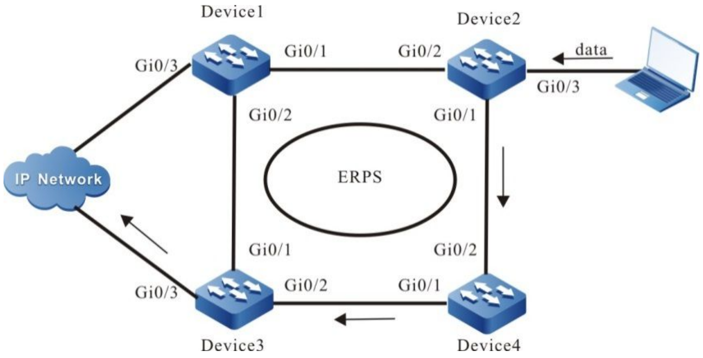


Table 71-1 Configure the ERPS Basic Functions

Configuration Steps

Step 1: Configure vlan and port link types.

#On Device1, create VLAN2, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2, vlan100~VLAN200 services to pass.

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

#On Device2, create VLAN2, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2, vlan100~VLAN200 services to pass.

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
```

```
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

#On Device3, create VLAN2, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2, vlan100~VLAN200 services to pass.

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

#On Device4, create VLAN2, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2, vlan100~VLAN200 services to pass.

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

Step 2: Configure the MST instance.

#On Device1, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
```

```
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#On Device2, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#On Device3, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#On Device4, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

Step 3: Configure ERPS.

#On Device1, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the owner port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device1# configure terminal
Device1(config)#erps ring 1
Device1(config-erps1)# control vlan 2
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2 rpl owner
Device1(config-erps1)# instance 1
Device1(config-erps1)# erps enable
Device1(config-erps1)# exit
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no shutdown
Device1(config-if-gigabitethernet0/1)# end
```

#On Device2, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device2# configure terminal
```

```
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/1
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 1
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

#On Device3, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the neighbour port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1 rpl neighbor
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end
```

#On Device4, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2
Device4(config-erps1)# instance 1
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

Step 4: Check the result.

#After the network topology gets stabilized, view the ERPS information of each device. Take device1 as an example:

#Query the ERPS information of Device1.

```
Device1# show erps ring 1 detail
Ring ID       : 1
Version       : v2
R-APS mel     : 7
Instance      :  1  vlans mapped : 100-200
Control VLAN  : 2
Node role     : Owner
Node state    : idle
Guard timer   :   500 ms         Running : 0 ms
Holdoff timer :     0 ms         Running : 0 ms
WTR timer     :     5 min        Running : 0 s
WTB timer     :     7 s          Running : 0 s
Subring       : No
Tc-limit enable    : No
Tc-limit Interval  : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/1 Flush Logic
   Remote Node ID : 0000-0000-0000
   Remote BPR     : 0
Gigabitethernet0/1 track CFM
   MD Name   :
   MA Name   :
   MEP ID    : 0
   RMEP ID   : 0
   CFM State : 0
Gigabitethernet0/2 Flush Logic
   Remote Node ID : 0000-0000-0000
   Remote BPR     : 0
Gigabitethernet0/2 track CFM
   MD Name   :
   MA Name   :
   MEP ID    : 0
   RMEP ID   : 0
   CFM State : 0
```

```
Port    Name                            PortRole   SwitchType PortStatus SignalStatus
--------------------------------------------------------------------------------------------
Port0   gigabitethernet0/1                Normal     --       Forwarding  Non-failed
Port1   gigabitethernet0/2                 Owner     --       Blocking   Non-failed
```

NOTE

- Before configuring ERPS, ensure that the link state of at least one point in the ring network is down, otherwise it will lead to looping.

71.3.2 Configure ERPS Load *-B -S -E -A*

Network Requirements

- All devices are in the same layer 2 network.
- Data traffic of Data1 is transmitted through device2-device1, and data traffic of Data2 is transmitted through device4-device3 to realize load sharing and provide link backup.

Network Topology

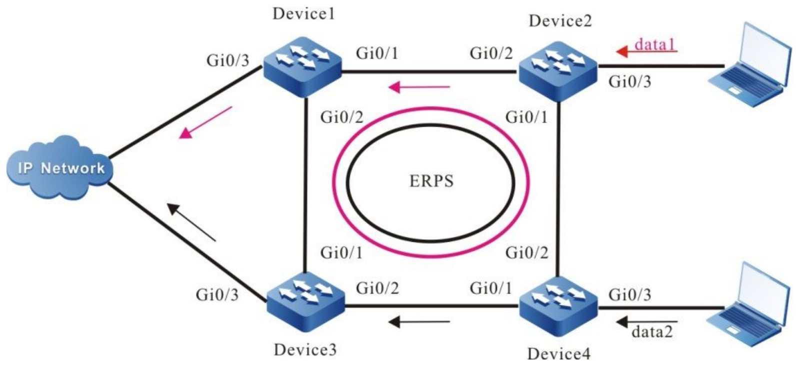


Figure 71-2 Configure ERPS Load

Configuration Steps

Step 1: Configure vlan and port link types.

#On Device1, create VLAN2~VLAN3, VLAN100~VLAN200, VLAN300~VLAN400, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2~VLAN3, vlan100~VLAN200, VLAN300~VLAN400 services to pass.

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
```

```
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device1(config-if-gigabitethernet0/1)#end
```

#On Device2, create VLAN2~VLAN3, VLAN100~VLAN200, VLAN300~VLAN400, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2~VLAN3, vlan100~VLAN200, VLAN300~VLAN400 services to pass.

```
Device2#configure terminal
Device2(config)#vlan 2,100-200
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#shutdown
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)# interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device2(config-if-gigabitethernet0/1)#end
```

#On Device3, create VLAN2~VLAN3, VLAN100~VLAN200, VLAN300~VLAN400, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2~VLAN3, vlan100~VLAN200, VLAN300~VLAN400 services to pass.

```
Device3#configure terminal
Device3(config)#vlan 2,100-200
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
```

```
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device3(config-if-gigabitethernet0/1)#end
```

#On Device4, create VLAN2~VLAN3, VLAN100~VLAN200, VLAN300~VLAN400, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2~VLAN3, vlan100~VLAN200, VLAN300~VLAN400 services to pass.

```
Device4#configure terminal
Device4(config)#vlan 2,100-200
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device4(config-if-gigabitethernet0/1)#exit
Device4(config)# interface gigabitethernet 0/2
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device4(config-if-gigabitethernet0/1)#end
```

Step 2: Configure the MST instance.

#On Device1, configure MST instance1 to map vlan100-200, MST instance2 to map vlan300-400, and activate the instance.

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# instance 2 vlan 300-400
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#On Device2, configure MST instance1 to map vlan100-200, MST instance2 to map vlan300-400, and activate the instance.

```
Device2#configure terminal
Device2(config)# spanning-tree mst configuration
Device2(config-mst)# instance 1 vlan 100-200
Device2(config-mst)# instance 2 vlan 300-400
Device2(config-mst)# active configuration pending
Device2(config-mst)#end
```

#On Device3, configure MST instance1 to map vlan100-200, MST instance2 to map vlan300-400, and activate the instance.

```
Device3#configure terminal

Device3(config)# spanning-tree mst configuration

Device3(config-mst)# instance 1 vlan 100-200

Device3(config-mst)# instance 2 vlan 300-400

Device3(config-mst)# active configuration pending

Device3(config-mst)#end
```

#On Device4, configure MST instance1 to map vlan100-200, MST instance2 to map vlan300-400, and activate the instance.

```
Device4#configure terminal

Device4(config)# spanning-tree mst configuration

Device4(config-mst)# instance 1 vlan 100-200

Device4(config-mst)# instance 2 vlan 300-400

Device4(config-mst)# active configuration pending

Device4(config-mst)#end
```

Step 3: Configure ERPS.

#On Device1, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device1# configure terminal

Device1(config)#erps ring 1

Device1(config-erps1)# control vlan 2

Device1(config-erps1)# port0 interface g0/1

Device1(config-erps1)# port1 interface g0/2

Device1(config-erps1)# instance 1

Device1(config-erps1)# erps enable

Device1(config-erps1)# end
```

#On Device1, configure ERPS ring2, configure vlan3 as the control vlan of ring2, configure gigabitothernet0/1 as the normal port of ring2, gigabitothernet0/2 as the normal port of ring2, and instance2 as data vlan of ring2, and enable the ERPS function of ring2.

```
Device1# configure terminal

Device1(config)#erps ring 2

Device1(config-erps1)# control vlan 3

Device1(config-erps1)# port0 interface g0/1

Device1(config-erps1)# port1 interface g0/2

Device1(config-erps1)# instance 2

Device1(config-erps1)# erps enable

Device1(config-erps1)# exit

Device1(config)# interface gigabitethernet 0/1
```

```
Device1(config-if-gigabitethernet0/1)#no shutdown
Device1(config-if-gigabitethernet0/1)# end
```

#On Device2, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the owner port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/1 rpl owner
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 1
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
```

#On Device2, configure ERPS ring2, configure vlan3 as the control vlan of ring1, configure gigabitothernet0/1 as the neighbour port of ring2, gigabitothernet0/2 as the normal port of ring2, and instance2 as data vlan of ring2, and enable the ERPS function of ring2.

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 3
Device2(config-erps1)# port0 interface g0/1 rpl neighbor
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 2
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

#On Device3, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1 rpl neighbor
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
```

#On Device3, configure ERPS ring2, configure vlan3 as the control vlan of ring2, configure gigabitothernet0/1 as the normal port of ring2, gigabitothernet0/2 as the normal port of ring2, and instance2 as data vlan of ring2, and enable the ERPS function of ring2.

```
Device3# configure terminal
Device3(config)#erps ring 2
Device3(config-erps1)# control vlan 3
Device3(config-erps1)# port0 interface g0/1
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 2
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end
```

#On Device4, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the neighbour port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2 rpl neighbour
Device4(config-erps1)# instance 1
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
```

#On Device4, configure ERPS ring2, configure vlan3 as the control vlan of ring2, configure gigabitothernet0/1 as the normal port of ring2, gigabitothernet0/2 as the owner port of ring2, and instance2 as data vlan of ring2, and enable the ERPS function of ring2.

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2 rpl owner
Device4(config-erps1)# instance 2
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

Step 4: Check the result.

#After the network topology gets stabilized, view the ERPS information of each device. Take device2 as an example:

#View the ERPS information of Device2.

```
Device2# show erps ring 1 detail
Ring ID       : 1
Version       : v2
R-APS mel     : 7
Instance      :  1  vlans mapped : 100-200
Control VLAN  : 2
Node role     : Owner
Node state    : idle
Guard timer   :   500 ms        Running : 0 ms
Holdoff timer :     0 ms        Running : 0 ms
WTR timer     :     5 min       Running : 0 s
WTB timer     :     7 s         Running : 0 s
Subring       : No
Tc-limit enable    : No
Tc-limit Interval  : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/1 Flush Logic
   Remote Node ID : 0000-0000-0000
   Remote BPR     : 0
Gigabitethernet0/1 track CFM
   MD Name   :
   MA Name   :
   MEP ID    : 0
   RMEP ID   : 0
   CFM State : 0
Gigabitethernet0/2 Flush Logic
   Remote Node ID : 0000-0000-0000
   Remote BPR     : 0
Gigabitethernet0/2 track CFM
   MD Name   :
   MA Name   :
   MEP ID    : 0
   RMEP ID   : 0
   CFM State : 0
Port    Name                        PortRole   SwitchType PortStatus SignalStatus
-------------------------------------------------------------------------------------------
Port0   gigabitethernet0/1            Owner      --        Blocking     Non-failed
```

```
Port1   gigabitethernet0/2                  Normal     --        Forwarding   Non-failed

Device2# show erps ring 2 detail
Ring ID       : 2
Version       : v2
R-APS mel     : 7
Instance      :  1  vlans mapped : 100-200
Control VLAN  : 3
Node role     : Neighbour
Node state    : idle
Guard timer   :   500 ms         Running : 0 ms
Holdoff timer :     0 ms         Running : 0 ms
WTR timer     :     5 min        Running : 0 s
WTB timer     :     7 s          Running : 0 s
Subring       : No
Tc-limit enable    : No
Tc-limit Interval  : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/1 Flush Logic
   Remote Node ID : 0000-0000-0000
   Remote BPR     : 0
Gigabitethernet0/1 track CFM
   MD Name   :
   MA Name   :
   MEP ID    : 0
   RMEP ID   : 0
   CFM State : 0
Gigabitethernet0/2 Flush Logic
   Remote Node ID : 0000-0000-0000
   Remote BPR     : 0
Gigabitethernet0/2 track CFM
   MD Name   :
   MA Name   :
   MEP ID    : 0
   RMEP ID   : 0
   CFM State : 0
Port    Name                               PortRole   SwitchType PortStatus SignalStatus
```

```
--------------------------------------------------------------------------------------------
Port0   gigabitethernet0/1              Neighbour    --      Blocking    Non-failed
Port1   gigabitethernet0/2              Normal       --     Forwarding   Non-failed
```

NOTE

- Under load, multiple logical rings on the same physical ring cannot be configured with the same data instance.

71.3.3 Configure ERPS Intersecting Ring *-B -S -E -A*

Network Requirements

- All devices are in the same layer 2 network.
- Device1-device2-device4-device3 and device3-device5-device6-device4 form two physical loops respectively, and all devices enable ERPS to break the link loop.

Network Topology

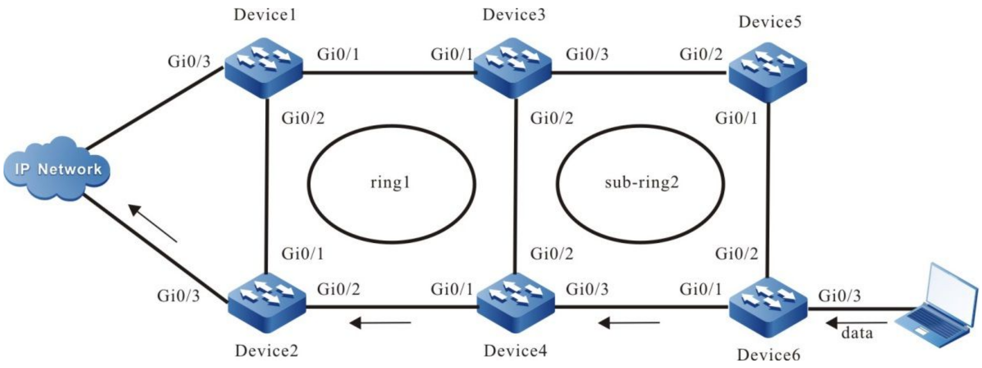


Figure 71-3 Configure the ERPS Intersecting Ring

Configuration Steps

Step 1: Configure vlan and port link types.

#On Device1, create VLAN2, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2, vlan100~VLAN200 services to pass.

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
```

```
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

#On Device2, create VLAN2, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2, vlan100~VLAN200 services to pass.

```
Device2#configure terminal
Device2(config)#vlan 2,100-200
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#shutdown
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)# interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)#end
```

#On Device3, create VLAN2~VLAN3, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2, vlan100~VLAN200 services to pass; configure the link type of port gigabitethernet0/3 as Trunk, allow VLAN3, vlan100~VLAN200 services to pass.

```
Device3#configure terminal
Device3(config)#vlan 2,100-200
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)#end
Device3(config)# interface gigabitethernet 0/3
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
```

```
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)#exit
```

#On Device4, create VLAN2~VLAN3, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN2, vlan100~VLAN200 services to pass; configure the link type of port gigabitethernet0/3 as Trunk, allow VLAN3, vlan100~VLAN200 services to pass.

```
Device4#configure terminal
Device4(config)#vlan 2,100-200
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)#exit
Device4(config)# interface gigabitethernet 0/2
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)#end
Device4(config)# interface gigabitethernet 0/3
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device4(config-if-gigabitethernet0/1)#exit
```

#On Device5, create VLAN3, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN3, vlan100~VLAN200 services to pass.

```
Device5#configure terminal
Device5(config)#vlan 2,100-200
Device5(config)# interface gigabitethernet 0/1
Device5(config-if-gigabitethernet0/1)#shutdown
Device5(config-if-gigabitethernet0/1)# switchport mode trunk
Device5(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device5(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device5(config-if-gigabitethernet0/1)#exit
Device5(config)# interface gigabitethernet 0/2
Device5(config-if-gigabitethernet0/1)# switchport mode trunk
Device5(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device5(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
```

```
Device5(config-if-gigabitethernet0/1)#end
```

#On Device6, create VLAN3, VLAN100~VLAN200, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, and allow VLAN3, vlan100~VLAN200 services to pass.

```
Device3#configure terminal
Device3(config)#vlan 3,100-200
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)#end
```

Step 2: Configure the MST instance.

#On Device1, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#On Device2, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device2#configure terminal
Device2(config)# spanning-tree mst configuration
Device2(config-mst)# instance 1 vlan 100-200
Device2(config-mst)# active configuration pending
Device2(config-mst)#end
```

#On Device3, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device3#configure terminal
Device3(config)# spanning-tree mst configuration
Device3(config-mst)# instance 1 vlan 100-200
Device3(config-mst)# active configuration pending
Device3(config-mst)#end
```

#On Device4, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device4#configure terminal
Device4(config)# spanning-tree mst configuration
Device4(config-mst)# instance 1 vlan 100-200
```

```
Device4(config-mst)# active configuration pending
Device4(config-mst)#end
```

#On Device5, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device5#configure terminal
Device5(config)# spanning-tree mst configuration
Device5(config-mst)# instance 1 vlan 100-200
Device5(config-mst)# active configuration pending
Device5(config-mst)#end
```

#On Device6, configure MST instance1 to map vlan100-200 and activate the instance.

```
Device6#configure terminal
Device6(config)# spanning-tree mst configuration
Device6(config-mst)# instance 1 vlan 100-200
Device6(config-mst)# active configuration pending
Device6(config-mst)#end
```

Step 3: Configure ERPS.

#On Device1, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the owner port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device1# configure terminal
Device1(config)#erps ring 1
Device1(config-erps1)# control vlan 2
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2 rpl owner
Device1(config-erps1)# instance 1
Device1(config-erps1)# erps enable
Device1(config-erps1)# end
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no shutdown
Device1(config-if-gigabitethernet0/1)# end
```

#On Device2, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the neighbour port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/1 rpl neighbour
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 1
```

```
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

#On Device3, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

#On Device3, configure ERPS ring2, configure vlan3 as the control vlan of ring2, configure gigabitothernet0/3 as the normal port of ring2, instance1 as data vlan of ring2, and ring2 as sub-ring, and enable the ERPS function of ring2.

```
Device3# configure terminal
Device3(config)#erps ring 2
Device3(config-erps1)# control vlan 3
Device3(config-erps1)# port0 interface g0/3
Device3(config-erps1)# instance 1
Device3(config-erps1)# sub-ring
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/3
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end
```

#On Device4, configure ERPS ring1, configure vlan2 as the control vlan of ring1, configure gigabitothernet0/1 as the normal port of ring1, gigabitothernet0/2 as the normal port of ring1, and instance1 as data vlan of ring1, and enable the ERPS function of ring1.

```
Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2
```

```
Device4(config-erps1)# instance 1

Device4(config-erps1)# erps enable

Device4(config-erps1)# exit

Device4(config)# interface gigabitethernet 0/1

Device4(config-if-gigabitethernet0/1)#no shutdown

Device4(config-if-gigabitethernet0/1)# end
```

#On Device4, configure ERPS ring2, configure vlan3 as the control vlan of ring2, configure gigabitothernet0/3 as the normal port of ring2, instance1 as data vlan of ring2, and ring2 as sub-ring, and enable the ERPS function of ring2.

```
Device4# configure terminal

Device4(config)#erps ring 2

Device4(config-erps1)# control vlan 3

Device4(config-erps1)# port0 interface g0/3

Device4(config-erps1)# instance 1

Device4(config-erps1)# sub-ring

Device4(config-erps1)# erps enable

Device4(config-erps1)# exit

Device4(config)# interface gigabitethernet 0/3

Device4(config-if-gigabitethernet0/1)#no shutdown

Device4(config-if-gigabitethernet0/1)# end
```

#On Device5, configure ERPS ring2, configure vlan3 as the control vlan of ring2, configure gigabitothernet0/2 as the normal port of ring2, gigabitothernet0/1 as the owner port of ring2, and instance1 as data vlan of ring2, and ring2 as sub-ring, and enable the ERPS function of ring2.

```
Device4# configure terminal

Device4(config)#erps ring 2

Device4(config-erps1)# control vlan 3

Device4(config-erps1)# port0 interface g0/1 rpl owner

Device4(config-erps1)# port0 interface g0/2

Device4(config-erps1)# instance 1

Device4(config-erps1)# sub-ring

Device4(config-erps1)# erps enable

Device4(config-erps1)# exit

Device4(config)# interface gigabitethernet 0/1

Device4(config-if-gigabitethernet0/1)#no shutdown

Device4(config-if-gigabitethernet0/1)# end
```

#On Device6, configure ERPS ring2, configure vlan3 as the control vlan of ring2, configure gigabitothernet0/2 as the neighbour port of ring2, gigabitothernet0/1 as the normal port of ring2, and instance1 as data vlan of ring2, and ring2 as sub-ring, and enable the ERPS function of ring2.

```
Device4# configure terminal

Device4(config)#erps ring 2

Device4(config-erps1)# control vlan 3
```

```
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port0 interface g0/2 rpl neighbour
Device4(config-erps1)# instance 1
Device4(config-erps1)# sub-ring
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

Step 4: Check the result.

#After the network topology gets stabilized, view the ERPS information of each device. Take device3 as an example:

#View the ERPS information of Device2.

```
Device3# show erps ring 1 detail
Ring ID       : 1
Version       : v2
R-APS mel     : 7
Instance      :  1  vlans mapped : 100-200
Control VLAN  : 2
Node role     : Normal
Node state    : idle
Guard timer   :   500 ms        Running : 0 ms
Holdoff timer :     0 ms        Running : 0 ms
WTR timer     :     5 min       Running : 0 s
WTB timer     :     7 s         Running : 0 s
Subring       : No
Tc-limit enable    : No
Tc-limit Interval  : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/1 Flush Logic
  Remote Node ID : 0000-0000-0000
  Remote BPR     : 0
Gigabitethernet0/1 track CFM
  MD Name   :
  MA Name   :
  MEP ID    : 0
```

```
    RMEP ID   : 0
    CFM State : 0
Gigabitethernet0/2 Flush Logic
    Remote Node ID : 0000-0000-0000
    Remote BPR     : 0
Gigabitethernet0/2 track CFM
    MD Name   :
    MA Name   :
    MEP ID    : 0
    RMEP ID   : 0
    CFM State : 0
Port    Name                           PortRole   SwitchType PortStatus SignalStatus
---------------------------------------------------------------------------------------------
Port0   gigabitethernet0/1                 Normal      --        Forwarding   Non-failed
Port1   gigabitethernet0/2                 Normal      --        Forwarding   Non-failed

Device2# show erps ring 2 detail
Ring ID       : 2
Version       : v2
R-APS mel     : 7
Instance      :  1  vlans mapped : 100-200
Control VLAN  : 3
Node role     : Normal
Node state    : idle
Guard timer   :   500 ms        Running : 0 ms
Holdoff timer :     0 ms        Running : 0 ms
WTR timer     :     5 min       Running : 0 s
WTB timer     :     7 s         Running : 0 s
Subring       : No
Tc-limit enable    : No
Tc-limit Interval  : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/3 Flush Logic
    Remote Node ID : 0000-0000-0000
    Remote BPR     : 0
Gigabitethernet0/1 track CFM
    MD Name   :
```

```
    MA Name   :
    MEP ID    : 0
    RMEP ID   : 0
    CFM State : 0
Port    Name                          PortRole   SwitchType PortStatus SignalStatus
-----------------------------------------------------------------------------------------------
Port0   gigabitethernet0/3            Normal        --         Forwarding   Non-failed
```

72 Network Test and Fault Diagnosis

72.1 Overview

With the network test and fault diagnosis tool, we can check the network connection status and diagnose the system fault. In daily maintenance, when it is necessary to check the network connection, we can use the ping function and traceroute function. When it is necessary to diagnose the system fault, we can open the system debugging information to diagnose the system fault.

72.2 Network Test and Fault Diagnosis Application

Table 72-1 Application List of Network Test and Fault Diagnosis

Application functions	
Ping function	ping
	ping ip
	Interactive ping
	grouping
Traceroute function	traceroute
	Interactive traceroute
System debugging function	System debugging

72.2.1 ping Function *-B -S -E -A*

The ping function is used to check the network connection status and whether the host is reachable. The ping function sends the ICMP echo request packet to the host and waits for the ICMP echo response, used to judge whether the destination is reachable. Ping can test the turnaround time from the source to the destination.

Configuration Conditions

None

ping

Table 72-2 ping

Step	Command	Description
Check whether the specified destination address is reachable	**ping** [**vrf** *vrf-name*] { *host-name* | *ip-address* } [**-l** *packet-length*] [**-w** *wait-time*] [**-n** *packet-number* | **-t**] [-s *src-ip-address*]	Mandatory

ping ip

Table 72-3 ping ip

Step	Command	Description
Check whether the specified destination address is reachable	**ping ip** { *host-name* | *ip-address* }	Mandatory The command can only be used for the most simple destination reachability check and there is no optional parameter.

Interactive ping

Table 72-4 Interactive ping

Step	Command	Description
Enter the ping interactive mode	**ping** [**vrf** *vrf-name*]	Mandatory In the privileged user mode, execute the command to enter the ping interactive mode.
Configure the network protocol type	**Protocol** [**ip**]:[**ip**]	Optional By default, Use the IPv4 protocol. Currently, only support the IPv4 protocol.
Configure the destination IP address or host name	**Target IP address or hostname**:{ *ip-address* | *host-name* }	Mandatory

Step	Command	Description
Configure the times of sending the ICMP request packet	**Repeat count** [**5**]:[*repeat-count*]	Optional By default, send for 5 times.
Configure the length of the ICMP request packet	**Datagram size** [**76**]:[*datagram-size*]	Optional The packet length is the size of the whole IP packet. By default, the packet length is 76 bytes.
Configure the timeout for waiting for the ICMP response	**Timeout in seconds** [**2**]:[*timeout*]	Optional By default, time out for 2s.
Enable the extended option	**Extended commands** [**no**]:[**yes** | **no**]	Optional After enabling the extended option, the configuration command of the extended option is available. By default, do not enable the extended option.
Configure the extended option, the source IP address or egress interface of the ICMP request packet	**Source address or interface:**{ *ip-address* | *interfacename* }	Optional After enabling the extended option, the command can be configured. By default, do not specify the source address and egress interface of the request packet.
Configure the extended selection, the service type of the ICMP request packet	**Type of service** [**0**]:[*tos*]	Optional After enabling the extended option, the command can be configured.

Step	Command	Description
		By default, the TOS value is 0.
Configure the extended option, setting not permitting the fragment	**Set DF bit in IP header?** [**no**]:[**yes | no**]	Optional After enabling the extended option, the command can be configured. By default, do not set the DF flag, permitting fragment.
Configure the extended option, validating the data content of the response packet	**Validate reply data?** [**no**]:[**yes | no**]	Optional After enabling the extended option, the command can be configured. By default, do not validate the data content.
Configure the extended option, the data content of the ICMP request packet	**Data pattern** [**abcd**]:[*data-pattern*]	Optional After enabling the extended option, the command can be configured. By default, the data content profile is “abcd”.
Configure the extended option, loose source route option, strict source route option, record route, record timestamp, display details	**Loose, Strict, Record, Timestamp, Verbose**[**none**]:[**l | s**] [**r / t / v**]	Optional After enabling the extended option, the command can be configured. By default, do not configure the extended option.
Enable scanning the sent ICMP request packet	**Sweep range of sizes** [**no**]:[**yes | no**]	Optional By default, scanning the sent packet is disabled.

Step	Command	Description
Configure the start value of the scanning	**Sweep min size** [**36**]:[*min-szie*]	Optional After enabling scanning the sent packet, the command can be configured. By default, the start value of the scanning is 36.
Configure the end value of the scanning	**Sweep max size** [**18024**]:[*max-size*]	Optional After enabling scanning the sent packet, the command can be configured. By default, the end value of the scanning is 18024
Configure the scanning incremental value	**Sweep interval** [**1**]:[*interval*]	Optional After enabling scanning the sent packet, the command can be configured. By default, the scanning incremental value is 1.

groupping

Table 72-5 groupping

Step	Command	Description
Send multiple groups of ICMP request packets, checking whether the destination address is reachable	**groupping** { *hostname* | *ip-address* } [[**-l** *packet-length*] [**-g** *packet-group*] [**-w** *wait-time*] [**-n** *packet-number*] [**-t**]	Mandatory

NOTE

- When pinging the destination host name, first configure the DNS function. Otherwise, ping fails. For DNS configuration, refer to “DNS Configuration” in “IP Network Protocol Configuration”.

72.2.2 traceroute Function *-B -S -E -A*

The traceroute function is used to view the gateways passed by the packet from the source to the destination. It is mainly used to check whether the destination is reachable and analyze the faulty network node. The executing process of traceroute is: First send one IP packet with TTL 1 to the destination host; the first-hop gateway drops the packet and returns one ICMP timeout error packet. In this way, traceroute gets the first gateway address in the path. And then traceroute sends one packet with TTL 2. In this way, get the address of the second-hop gateway. Continue the process until reaching the destination host. The UDP port number of the traceroute packet is the port number of the destination that cannot be used by any application program. After the destination receives the packet, return one error packet of the port unreachable. In this way, get all gateway addresses on the path.

Configuration Conditions

None

traceroute

Table 72-6 traceroute

Step	Command	Description
View the gateways passed by the packet from the source to the destination	**traceroute** [**ip** | **vrf** *vrf-name*] { *hostname* | *ip-address* }	Mandatory

Interactive traceroute

Table 72-7 Interactive traceroute

Step	Command	Description
Enter the traceroute interactive mode	**traceroute** [**vrf** *vrf-name*]	Mandatory In the privileged user mode, execute the command to enter the traceroute interactive mode.
Configure the network protocol type	**Protocol** [**ip**]:[**ip**]	Optional

Step	Command	Description
		By default, Use the IPv4 protocol. Currently, only support the IPv4 protocol.
Configure the destination IP address or host name	**Target IP address or hostname**:{ *ip-address* | *host-name* }	Mandatory
Configure the source IP address or egress interface of the traceroute packet	**Source address or interface**:{ *ip-address* | *interface-name* }	Optional By default, do not specify the source IP address or egress interface of the packet
Configure the timeout for waiting for each detection packet response	**Timeout in seconds** [**3**]:*timeout*	Optional By default, time out after 3s.
Configure the times of sending the detection packet with the same TTL value	**Probe count** [**3**]:*probe-count*	Optional By default, send for three times.
Configure the minimum TTL value of the detection packet	**Minimum Time to Live** [**1**]:*min-ttl*	Optional By default, the minimum TTL value is 1.
Configure the maximum TTL value of the detection packet	**Maximum Time to Live** [**30**]:*max-ttl*	Optional By default, the maximum TTL value is 30.
Configure the destination UDP port number of the detection packet	**Port Number** [**33434**]:*port-number*	Optional By default, the destination port number is 33434.
Configure the extended option, loose source route option, strict source route option,	**Loose, Strict, Record, Timestamp, Verbose**[**none**]:[**l | s**] [**r / t / v**]	Optional By default, do not configure the option.

Step	Command	Description
record route, record timestamp, display details		

72.2.3 System Debugging Function *-B -S -E -A*

To help the user diagnose the problem, the most function modules of the device provide the debugging function.

The debugging function has two switch controls:

- The debugging switch of the module, controlling whether to generate the debugging information of the module
- The output switch of the screen, controlling whether to output the debugging information to the terminal

Configuration Conditions

None

System Debugging

Table 72-8 System Debugging

Step	Command	Description
Open the output switch of the remote login system debugging screen	**terminal monitor**	Optional The remote login includes telnet, ssh and so on. By default, the switch is closed.
Enter the global configuration mode	**configure terminal**	-
Open the output switch of the console system debugging screen	**logging console**	Optional By default, the switch is opened.
Exit the global configuration mode	**exit**	-
Open the debugging switch of the system function module	**debug** { **all** | *module-name* [*option*] }	Optional By default, all debugging switches of the system

Step	Command	Description
		function modules are closed.

NOTE

- The debugging information can be displayed on the terminal only after configuring **debug** module-name option, **terminal monitor** or **logging console** at the same time.
- The generating and output of the debugging information affect the system performance, so when it is necessary, had better use the **debug** module-name option command to open the specified debugging switch. The **debug all** command opens all debugging switches, so we had better not use. After debugging ends, close the corresponding debugging switch in time or use the **no debug all** command to close all debugging switches.

72.2.4 Monitoring and Maintaining of Network Test and Fault Diagnosis

-B -S -E -A

Table 72-9 Monitoring and Maintaining of the System Test and Fault Diagnosis

Command	Description
show debugging	Display the function module information of the opened debugging switch in the system.

72.3 Typical Configuration Example of Network Test and Fault Diagnosis

72.3.1 ping Application ***-B -S -E -A***

Network Requirements

- Device1 fails to use telnet to log into Device3 and we need to confirm whether the route between Device1 and Device3 is reachable.

Network Topology

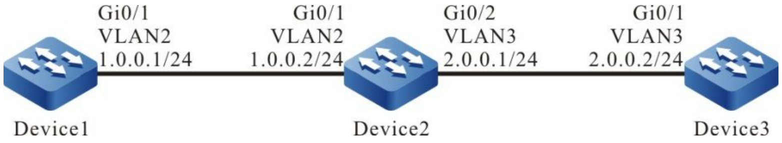


Figure 72-1 ping Application Networking

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Use the ping command to view whether the route between Device1 and Device3 is reachable.

#View whether Device1 and Device3 can ping each other.

```
Device1#ping 2.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

Step 4: Use the ping command to view whether the route between Device1 and Device2 is reachable.

#View whether Device1 and Device2 can ping each other.

```
Device1#ping 1.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

Step 5: Use the ping command to view whether the route between Device2 and Device3 is reachable.

#View whether Device2 and Device3 can ping each other.

```
Device2#ping 2.0.0.2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

From the above result, we can see that Device1 and Device2 can communicate with each other, Device2 and Device3 can communicate with each other, and the problem appears between Device1 and Device3. Later, we can check the route configuration, or use the **debug ip icmp** command to view whether the packet content is correct. We also can use traceroute described in the next section to confirm the faulty network node.

72.3.2 traceroute Application *-B -S -E -A*

Network Requirements

- Device1 fails to use telnet to log into Device3 and we need to confirm whether the route between Device1 and Device3 is reachable. If the route is unreachable, we need to confirm the fault of the network node.

Network Topology

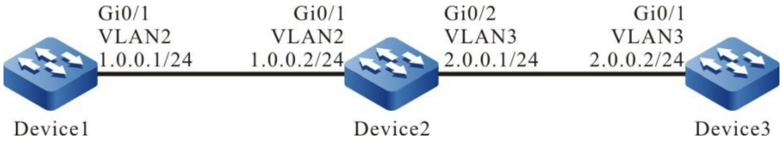


Figure 72-2 traceroute Application Networking

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Use the **traceroute** command to view whether the route between Device1 and Device3 is reachable.

# View whether Device1 and Device3 can ping each other.

```
Device1#traceroute  2.0.0.2
Type escape sequence to abort.
Tracing the route to 2.0.0.2 , min ttl = 1, max ttl = 30 .

 1  1.0.0.2    0 ms    0 ms    0 ms
 2  *  *       *
 3  *  *       *
 4  *  *       *
 5  *  *       *
 6
```

From the above result, the traceroute packet sent by Device1 can reach Device2. The traceroute packet from Device2 cannot reach Device3. Later, we need to check the route configuration between Device2 and Device3 and line, or use the **debug ip icmp** command to view whether the packet content is correct. We also can use ping described in the last section to detect the connection between Device2 and Device3.

73 Keepalive Gateway

73.1 Overview

Keepalive gateway sets the Ethernet interface to send the keepalive packet to the specified gateway address, used to monitor the reachability of the destination gateway. When the gateway is unreachable, close the interface IP protocol layer.

After configuring the keepalive gateway on one interface, the interface regularly sends the ARP request packet to the configured gateway address. When the interface does not receive the ARP response packet for successive N times (N is the retry times configured for the user), close the interface IP protocol layer. Until receiving the ARP response packet again, enable the interface IP protocol layer.

73.2 Gateway Keepalive Function Configuration

Table 73–1 Gateway Keepalive Function Configuration List

Configuration Task	
Configure the keepalive gateway function	Configure the keepalive gateway basic function
	Configure the sending parameters of the keepalive packet

73.2.1 Configure Gateway Keepalive Function *-S -E -A*

Configuration Conditions

Before configuring the gateway keepalive function, first complete the following task:

- Configure the IP address of the interface

Configure Gateway Keepalive Basic Function

Table 73–2 Configure the Gateway Keepalive Basic Function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the gateway keepalive	**keepalive gateway** *ip-address* [*interval* | **msec** *interval*] [*retry-count*]	Mandatory By default, do not enable the gateway keepalive function.

Configure Sending Parameters of Keepalive Packet

When configuring the sending parameters of the keepalive packet, we can control the sending rate of the gateway keepalive packet. When the sending rate of the keepalive packet reaches the configured value, pause for the configured time and then continue to send the keepalive packets.

Table 73–3 Configure the Sending Parameters of the Keepalive Packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the sending rate of the keepalive packet	**keepalive gateway disperse pkt-rate** *packet-rate*	Optional By default, the maximum sending rate of the keepalive packet is 100pps.
Configure the time of pausing sending the keepalive packet	**keepalive gateway disperse pause-time** *pause-time*	Optional By default, the time of pausing sending the keepalive packet is 100ms.

73.2.2 Monitoring and Maintaining of Gateway Keepalive *-S -E -A*

Table 73–4 Monitoring and Maintaining of Gateway Keepalive

Command	Description
clear keepalive gateway statistics [*interface-name*]	Clear the sending and receiving statistics information of the gateway keepalive

Command	Description
show keepalive gateway [*interface-name*]	View the interface enabled with the gateway keepalive and its configuration
show keepalive gateway disperse	View the sending parameter configuration of the gateway keepalive packet
show keepalive gateway statistics [*interface-name*]	View the statistics information of the gateway keepalive

73.3 Typical Configuration Example of Gateway Keepalive

73.3.1 Configure Gateway Keepalive *-S -E -A*

Network Requirements

- Device X is the connection device, just transmitting data transparently.
- Run the OSPF protocol on Device1, Device2 and Device3 to perform the route interacting.
- The data flow from Device1 to the 201.0.0.0/24 segment first selects Device3.
- The line between Device1 and Device3 uses the gateway keepalive function. When the line between Device1 and Device3 fails, the gateway keepalive fast detects the fault and modifies the interface status to down. After OSPF feels the status change of the interface, switch the route to Device2 for communication.

Network Topology

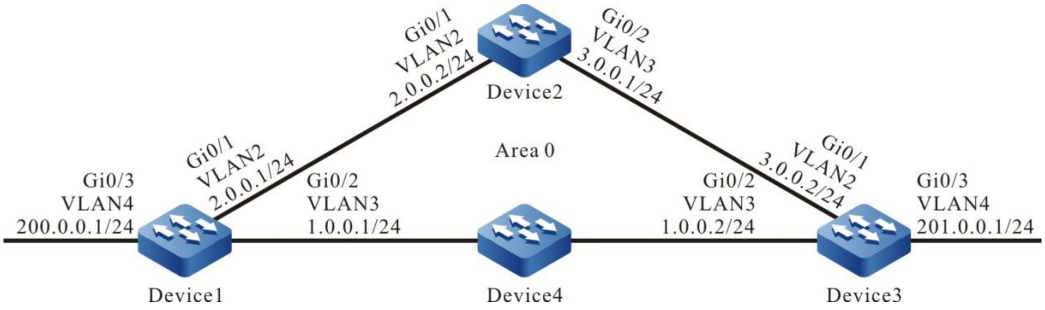


Figure 73–1 Networking of Configuring the Gateway Keepalive

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the OSPF process.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the route table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:20:17, vlan3
C   2.0.0.0/24 is directly connected, 13:01:32, vlan2
O   3.0.0.0/24 [110/2] via 2.0.0.2, 01:11:40, vlan2
               [110/2] via 1.0.0.2, 00:02:00, vlan3
C   200.0.0.0/24 is directly connected, 01:31:58, vlan4
O   201.0.0.0/24 [110/2] via 1.0.0.2, 00:02:00, vlan3
```

#The data flow from Device1 to the segment 201.0.0.0/24 first selects Device3.

NOTE

- The viewing method of Device2 and Device3 is the same as that of Device1, so the viewing process is omitted here.

Step 4: Configure the gateway keepalive.

#Configure Device1.

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#keepalive gateway 1.0.0.2
Device1(config-if-vlan3)#exit
```

#Configure Device3.

```
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#keepalive gateway 1.0.0.1
Device3(config-if-vlan3)#exit
```

#View the gateway keepalive information of Device1.

```
Device1#show keepalive gateway
interface vlan3 gateway 1.0.0.2 time 10s retry 3 remain 3 now UP
```

#View the gateway keepalive information of Device3.

```
Device3#show keepalive gateway
interface vlan3 gateway 1.0.0.1 time 10s retry 3 remain 3 now UP
```

Step 5: Check the result.

#After the line between Device1 and Device3 fails, the gateway keepalive fast detects the fault and modifies the interface VLAN3 status to down.

```
Device1#show keepalive gateway
interface vlan3 gateway 1.0.0.2 time 10s retry 3 remain 0 now DOWN
```

#After OSPF feels the status change of the interface VLAN3, switch the route to Device2 for communication.

```
Device1# show ip ospf interface vlan3
VLAN3 is down, line protocol is down
  OSPF is enabled, but not running on this interface

Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 13:16:40, vlan2
O   3.0.0.0/24 [110/2] via 2.0.0.2, 00:01:25, vlan2
C   200.0.0.0/24 is directly connected, 00:10:53, vlan4
O   201.0.0.0/24 [110/3] via 2.0.0.2, 00:00:18, vlan2
```

#We can see that the data flow from Device1 to the segment 201.0.0.1/24 first selects Device2.

74 SLA

74.1 Overview

SLA (Service Level Agreements) calculates the related parameters according to the packet transmission and outputs the report at last. SLA, also called RTR (Response Time Reporter), is one network detection and monitoring tool. SLA regularly sends the packets of the specified protocol to detect and monitor the network communication. SLA can diagnose different network applications and output the test result by configuring different types of RTR entities and adjusting.

SLA basic concepts:

- RTR Entity: RTR Entity is one universal concept and not related with the specific type of RTR entity. The current RTR entity types of the system include: the ICMP-echo entity, ICMP-path-echo entity, ICMP-path-jitter entity, and UDP-echo entity used to detect the network communication; the VoIP-jitter entity used to detect the network transmitting the VoIP packets; the FLOW-statistics entity used to detect the interface traffic; the MAC-ping entity used to detect the Ethernet link communication service quality.
- RTR Group: One RTR entity group is the set of one or multiple entities;
- RTR responder: The RTR responder is configured at the destination, mainly used to set up the connection with the source and respond the detection packet sent by the source. Most entities do not need to configure the responder, but when using the UDP-echo entity and VoIP-jitter entity, we should configure the responder.
- RTR Schedule: If only configuring the RTR entity or RTR entity group, we cannot detect, but should initiate the scheduling so that the detection can be completed.

74.2 SLA Function Configuration

Table 74-1 SLA Function Configuration List

Configuration Task	
Enable RTR	Enable RTR
Configure the RTR entity	Create the RTR entity
	Configure the ICMP-echo entity
	Configure the ICMP-path-echo entity
	Configure the ICMP-path-jitter entity

Configuration Task	
	Configure the VoIP-jitter entity
	Configure the UDP-echo entity
	Configure the MAC-ping entity
	Configure the FLOW-statistics entity
	Configure the common configuration of the entity
Configure the RTR entity group	Configure the RTR entity group
Configure the RTR responder	Configure the RTR responder
Configure the RTR schedule	Configure the RTR schedule
Configure pausing scheduling the entity	Configure pausing scheduling the entity
Configure restoring scheduling the entity	Configure restoring scheduling the entity

74.2.1 Enable RTR *-S -E -A*

In the configuration tasks of RTR, first enable RTR so that the configuration of the other functions can take effect.

Configuration Conditions

None

Enable RTR

Table 74-2 Enable RTR

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable RTR	**rtr enable**	Mandatory

Step	Command	Description
		By default, do not enable RTR.

74.2.2 Configure RTR Entity *-S -E -A*

Configuration Conditions

Before configuring the RTR entity, first complete the following task:

- Enable RTR.

Create RTR Entity

One entity corresponds to one type of detection. After creating the RTR entity and entering the entity configuration mode, we can configure the parameters of the entity.

Table 74-3 Create the RTR Entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the RTR entity	**rtr** *entity-id entity-type*	Mandatory

Configure ICMP-echo Entity

The ICMP-echo entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end. In one detection period, as long as the ICMP-echo entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status and history information in time and reduce inputting the common ping command frequently at the same time.

Table 74-4 Configure the ICMP-echo Entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the ICMP-echo entity configuration mode	**rtr** *entity-id* [**icmpecho**]	Mandatory

Step	Command	Description
Configure the detection attribute	**set** [**vrf** *vrf-name*] *target-ip-address* [*npacket*] [*data-size*] [*timeout*] [*frequency-value*] [**extend** *source-ip-address* [*tos*] [*set-DF*] [*verify-data*]]	Mandatory By default, do not configure the detection attribute of the entity.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

NOTE

- The scheduling interval of the ICMP-echo entity needs to meet the following requirement: scheduling interval > npacket * timeout
- If configuring the scheduler for the entity, the age time of the scheduler should be larger than the scheduling interval of the entity.

Configure ICMP-path-echo Entity

The ICMP-path-echo entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end, as well as the delay and packet loss between the detection end and the intermediate devices from the detection end to the destination. In one detection period, as long as the ICMP-path-echo entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status (for example, which network device on the path has serious delay) and history information in time.

Table 74-5 Configure the ICMP-path-echo Entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the ICMP-path-echo entity configuration mode	**rtr** *entity-id* [**icmp-path-echo**]	Mandatory

Step	Command	Description
Configure the detection attribute	**set dest-ipaddr** *target-ip-address* [**source-ipaddr** *source-ip-address*]	Mandatory
Configure the loose source route selection	**lsr-path** [*hop-ip-address-list* | **none**]	Optional By default, do not configure the loose source route selection.
Configure only detecting the network status from the source to the destination	**targetOnly** [**true | false**]	Optional By default, if targetOnly is true, only detect the network status from the source to the destination. If targetOnly is false, detect the network status from the source to the destination hop by hop.
Configure whether to verify the content of the response packet	**verify-data** [**true | false**]	Optional By default, do not verify the data content.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Configure ICMP-path-jitter Entity

The ICMP-path-jitter entity is to detect the network communication. It regularly sends the ICMP echo request packet to one destination address in the network, so as to get the delay, jitter, and packet loss of the packet transmission from the detection end to the destination end, as well as the delay, jitter and packet loss between the detection end and the intermediate devices from the detection end to the destination. In one detection period, as long as the ICMP-path-jitter entity receives one ICMP echo request response packet, the entity status is reachable.

The general network devices all support ping, so the entity can take effect in detecting the network communication. With the rich scheduling policies and log recording function, we can let the network administrator get to know the network communication status (for example, which network device on the path has serious delay) and history information in time.

Table 74-6 Configure the ICMP-path-jitter Entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the ICMP-path-jitter configuration mode	**rtr** *entity-id* [**icmp-path-jitter**]	Mandatory
Configure the detection attribute	**set dest-ipaddr** *target-ip-address* [*pkt-number*] [*pkt-interval*] [**source-ipaddr** *source-ip-address*]	Mandatory
Configure the IP address of the loose source route selection	**lsr-path** [*hop-ip-address-list* | **none**]	Optional By default, do not configure the loose source route selection.
Configure only detecting the network status from the source to the destination	**targetOnly** [**true** | **false**]	Optional By default, if targetOnly is true, only detect the network status from the source to the destination. If targetOnly is false, detect the network status from the source to the destination hop by hop.
Configure the jitter threshold and over-limit rule	**threshold-jitter** *jitter* **direction** { **be** | **se** }	Optional By default, the jitter threshold is 6000ms and the over-limit rule is be.
Configure whether to verify the content of the response packet	**verify-data** [**true** | **false**]	Optional By default, do not verify the data content.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

NOTE

- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.

Configure VoIP-jitter Entity

The VoIP-jitter entity is the RTR entity used to measure the transmission quality of the VoIP packet in the general IP network.

The VoIP-jitter entity can simulate the G.711 A Law, G.711 mu Law, and G.729A codec or the customized codes to send the UDP packet with the corresponding rate, packet interval and size from the source device to the destination device, measure the turnaround time, uni-directional packet loss and uni-directional delay of the packet, and calculates the ICPIF value based on the statistics information. At last, estimate the MOS value according to the ICPIF value. In the detection period, as long as the VoIP-jitter entity receives one detection response packet, the status of the entity is reachable.

Table 74-7 Configure the VoIP-jitter Entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the VoIP-jitter configuration mode	**rtr** *entity-id* [**jitter**]	Mandatory If the entity already exists, directly enter the entity configuration mode.
Configure the detection attribute	**set dest-ipaddr** *target-ip-address* **dest-port** *target-port* { **g711alaw** | **g711ulaw** | **g729a** | **user_defined** *packet-size packet-number packet-interval schedule-interval* } [**source-ipaddr** *source-ip-address*] [**source-port** *source-port*]	Mandatory
Configure the uni-directional delay threshold from the source to the destination and over-limit rule	**threshold-sd-delay** *sd-delay* **direction** { **be** | **se** }	Optional By default, the sd delay threshold is 5000ms and the over-limit rule is be.
Configure the uni-directional jitter threshold from the source to the	**threshold-sd-jitter** *sd-jitter* **direction** { **be** | **se** }	Optional

Step	Command	Description
destination and over-limit rule		By default, the sd jitter threshold is 6000ms and the over-limit rule is be.
Configure the packet loss threshold and over-limit rule from the source to the destination	**threshold-sd-pktloss** *sd-packet* **direction** { **be** | **se** }	Optional By default, the sd packet loss threshold is 60000 and the over-limit rule is be.
Configure the uni-directional delay threshold from the destination to the source and over-limit rule	**threshold-ds-delay** *ds-delay* **direction** { **be** | **se** }	Optional By default, the ds delay threshold is 5000ms and the over-limit rule is be.
Configure the uni-directional jitter threshold from the destination to the source and over-limit rule	**threshold-ds-jitter** *ds-jitter* **direction** { **be** | **se** }	Optional By default, the ds unit-directional jitter threshold is 6000ms and the over-limit rule is be.
Configure the packet loss threshold from the destination to the source and over-limit rule	**threshold-ds-pktloss** *ds-packet* **direction** { **be** | **se** }	Optional By default, the ds packet loss threshold is 60000 and the over-limit rule is be.
Configure the icpif threshold and the over-limit rule	**threshold-icpif** *icpif-value* **direction** { **be** | **se** }	Optional By default, the icpif threshold is 100000000 and the over-limit rule is be.
Configure the mos threshold and the over-limit rule	**threshold-mos** *mos-value* **direction** { **be** | **se** }	Optional By default, the mos threshold is 10000000 and the over-limit rule is be.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

NOTE

- When using the VoIP-jitter entity detection, besides configuring the VoIP-jitter entity, we also need to configure the RTR responder at the destination.
- By default, the VoIP-jitter entity sends many packets, which occupy the network bandwidth, so when configuring the entity exceeds one hour, the shell prompts.
- When the VoIP-jitter entity detects the network transmitting the VoIP packet, the clocks of the source and the destination need to be consistent, so before scheduling the VoIP-jitter entity, we also need to configure the NTP server at the destination and NTP client at the source. After the clocks are synchronized, configure the RTR responder, and at last, configure the scheduler. For the configuration of NTP, refer to NTP Configuration Manual.
- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.

Configure UDP-echo Entity

The UDP-echo entity mainly detects the UDP packet transmitted in the IP network. In the entity, we need to specify the destination address and port of the sent packet. We can monitor the transmission of the UDP packet in the IP network by scheduling the entity. In one detection period, as long as the UDP-echo entity receives one detection response packet, the entity status is reachable.

The UDP-echo entity can monitor efficiently to record the turnaround delay, packet loss and other information of the UDP packet in the IP network, even record the monitored history information by logs so that the network administrator can get to know the network communication and fix the fault.

Table 74-8 Configure the UDP-echo Entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the UDP-echo entity configuration mode	**rtr** *entity-id* [**udp-echo**]	Mandatory If the entity already exists, directly enter the entity configuration mode.
Configure the detection attribute	**set dest-ipaddr** *target-ip-address* **dest-port** *target-port* [**source-ipaddr** *source-ip-address*] [**source-port** *source-port*]	Mandatory
Configure the filling content of the packet	**data-pattern** *pad*	Optional By default, the filling content is “ABCD”.

Step	Command	Description
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

NOTE

- When using the UDP-echo entity detection, besides configuring the UDP-echo entity, we also need to configure the RTR responder at the destination.

Configure MAC-ping Entity

The MAC-ping entity is to detect the communication service quality of the Ethernet link. It regularly sends the detection packets to one destination MAC address or destination MEPID of the Ethernet link, so as to get the delay and packet loss of the packet transmission from the detection end to the destination end.

The MAC-ping entity needs the supporting of CFM (Connectivity Fault Management). Before configuring the MAC-ping entity, first need to configure the CFM maintenance domain, MEPID, service instance and other parameters.

Table 74-9 Configure the MAC-ping Entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the MAC-ping entity configuration mode	**rtr** *entity-id* [**macping**]	Mandatory If the entity already exists, directly enter the entity configuration mode.
Configure the detection attribute	**set** *maintenance-domain service-instance* { **dst-mac** *mac-address* | **dst-mepid** *dst-mepid* } [**src-mepid** *src-mepid*]	Mandatory By default, do not configure the detection attribute of the entity.
Configure the scheduling parameters of the entity	**cycle** *cycletime* **num-packes** *packetnum* **avg-cyclenum** *cyclenum* **sched-interval** *interval*	Optional

Step	Command	Description
Configure the entity name	**macping-name** *name*	Mandatory By default, do not configure the entity name.
Configure the number of the saved history records	**history-max-count** *count*	Optional By default, save one history record.
Configure the alarm threshold of the uni-directional delay	**avgdelay-alarm** *delaylarm*	Optional By default, the alarm threshold of the uni-directional delay is 500ms.
Configure the alarm threshold of the bi-directional delay	**avgrndtrpdelay-alarm** *rpdelaylarm*	Optional By default, the alarm threshold of the bi-directional delay is 500ms.
Configure the jitter alarm threshold	**avgjitter-alarm** *jitterlarm*	Optional By default, the jitter alarm threshold is 500ms.
Configure the alarm threshold of the packet loss	**avglost-alarm** *lostlarm*	Optional By default, the alarm threshold of the packet loss is 50%.

Configure FLOW-statistics Entity

The FLOW-statistics entity is to detect the interface traffic and one entity corresponds to one interface. We can monitor the traffic on the interface by scheduling the entity. In one detection period, as long as there are packets passing the interface monitored by the FLOW-statistics entity, the entity status is reachable.

The interval of the FLOW-statistics entity monitoring the interface traffic is 10s-10min. We can record the traffic peak value information on the interface by monitoring, even can record the history information of the traffic statistics during each monitoring, so as to make the network administrator get to know the network communication status and fix the fault.

Table 74-10 Configure the FLOW-statistics Entity

Step	Command	Description
Enter the system configuration mode	**configure terminal**	-
Enter the FLOW-statistics entity configuration mode	**rtr** *entity-id* [**flow-statistics**]	Mandatory If the entity already exists, directly enter the entity configuration mode.
Configure the detection attribute	**flow-statistics interface** *interface-name* **interval** *interval*	Mandatory
Configure the traffic threshold received by the interface and the over-limit rule	**threshold-inflow** *flow-value* **direction** { **be** | **se** }	Optional By default, the traffic threshold received by the interface is 200000000bps (bit/s) and the over-limit rule is be.
Configure the threshold of the packets received by the interface and the over-limit rule	**threshold-inpacket** *packet-value* **direction** { **be** | **se** }	Optional By default, the threshold of the packets received by the interface is 200000000 and the over-limit rule is be.
Configure the threshold of the traffic received by the interface and the over-limit rule	**threshold-outflow** *flow-value* **direction** { **be** | **se** }	Optional By default, the traffic threshold sent by the interface is 200000000 bps (bit/s) and the over-limit rule is be.
Configure the threshold of the packets received by the interface and over-limit rule	**threshold-outpacket** *packet-value* **direction** { **be** | **se** }	Optional By default, the threshold of the packets received by the interface is 200000000 and the over-limit rule is be.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

NOTE

- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.

Configure Common Configuration of Entities

Table 74-11 Configure the Common Configuration of the Entities

Step	Command	Description
Configure the alarm type	**alarm-type** [**log** | **log-and-trap** | **trap** | **none**]	Optional By default, the alarm mode is none, that is, do not alarm.
Configure the number of the saved history records	**number-of-history-kept** *history-number*	Optional By default, save one history record. The entity not supporting the command: MAC-ping entity
Configure the period of saving the history records	**periods** *periods*	Optional By default, after each scheduling ends, save one history record. The entity not supporting the command: MAC-ping entity
Configure the timeout	**timeout** *timeout*	Optional By default, the timeout is: ICMP-path-echo entity 5000ms ICMP-path-jitter entity 5000ms VoIP-jitter entity 50000ms UDP-echo entity 5000ms The entity not supporting the command: ICMP-echo entity FLOW-statistics entity MAC-ping entity

Step	Command	Description
Configure the TOS value of the packet	**tos** *tos-value*	Optional By default, the TOS value is 0. The entity not supporting the command: ICMP-echo entity LSP-ping entity FLOW-statistics entity MAC-ping entity
Configure the VRF attribute of the entity	**vrf** *vrf-name*	Optional By default, do not configure the VRF attribute of the entity. The entities not supporting the command: ICMP-echo entity FLOW-statistics entity MAC-ping entity
Configure the scheduling interval of the entity	**frequency** *seconds*	Optional By default, the scheduling interval is: ICMP-path-echo entity 60s ICMP-path-jitter entity 60s UDP-echo entity 60s The entities not supporting the command: ICMP-echo entity VoIP-jitter entity FLOW-statistics entity MAC-ping entity
Configure the length of the detection packet	**request-data-size** *data-size*	Optional By default, the length of the detection packet: ICMP-path-echo entity 70 bytes

Step	Command	Description
		ICMP-path-jitter entity 70 bytes UDP-echo entity 16 bytes The entities not supporting the command: ICMP-echo entity VoIP-jitter entity FLOW-statistics entity MAC-ping entity
Configure the packet loss threshold and the over-limit rule	**threshold-pktloss** *pktloss* **direction** { **be | se** }	Optional By default, the packet loss threshold: ICMP-echo entity 150 ICMP-path-echo entity 1 ICMP-path-jitter entity 100 UDP-echo entity 1 The over-limit rule is be. The entities not supporting the command: VoIP-jitter entity FLOW-statistics entity MAC-ping entity
Configure the bi-directional delay threshold and the over-limit rule	**threshold-rtt** *rtt* **direction** { **be | se** }	Optional By default, the bi-directional delay threshold is: ICMP-echo entity 9000ms ICMP-path-echo entity 9000ms ICMP-path-jitter entity 9000ms VoIP-jitter entity 9000ms UDP-echo entity 9000ms The over-limit rule is be.

Step	Command	Description
		The entities not supporting the command: FLOW-statistics entity MAC-ping entity

NOTE

- If the RTR entity already exists and the entity is in the un-scheduled state, execute the **rtr** *entity-id* command to enter the entity configuration mode directly.
- When the over-limit rule is be and the actual value is larger than or equal to the threshold, it judged as over-limit; when the over-limit rule is se and the actual value is smaller than or equal to the threshold, it is judged as over-limit.
- The scheduling interval of the ICMP-path-echo entity needs to meet the following requirement: scheduling interval > timeout.
- The scheduling interval of the ICMP-path-jitter entity needs to meet the following requirement: scheduling interval > timeout; timeout needs to meet the following requirement: timeout > pkt-number * pkt-interval; For the pkt-number parameter and the pkt-interval parameter, refer to the set command of the ICMP-path-echo entity.
- When the scheduling interval of the VoIP-jitter entity selects simulating G.711ALaw, G.711muLaw, and G.729A codec, it is necessary to meet the following requirement: scheduling interval > timeout + 5; when selecting the customized codec, it is necessary to meet the following requirement: scheduling interval > schedule-interval + 5; schedule-interval needs to meet the following requirement: schedule-interval > packet-number * packet-interval; for the schedule-interval, packet-number and packet-interval parameters, refer to the set command of the VoIP-jitter entity.
- The scheduling interval of the UDP-echo entity needs to meet the following requirement: scheduling interval > timeout + 5.

74.2.3 Configure RTR Entity Group *-S -E -A*

One RTR entity group is the set of one or multiple RTR entity groups. One RTR entity can belong to multiple RTR entity groups and the group cannot become the member of the group. One group can only contain one member once. The RTR entity group is identifies by the group ID uniquely and the group name is automatically generated by the system.

The RTR entity group is mainly to schedule one RTR set. The scheduling for the RTR entity group is equivalent to the scheduling for all RTR entities in the RTR entity group. The detection result is saved in the history records of the RTR entity.

Configuration Conditions

Before configuring the RTR entity group, first complete the following task:

- Enable RTR.

Configure RTR Entity Group

Table 74-12 Configure the RTR Entity Group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the configuration mode of the RTR entity group	**rtr group** *group-id*	Mandatory If the RTR entity group does not exist, automatically create the entity group.
Add the members in the RTR entity group	**member** *entity-list*	Optional By default, the RTR entity group does not contain any member.
Configure the options of the RTR entity group	**option** { **or** | **and** }	Optional By default, the status option of the RTR entity group is and (when all entities in the group are reachable, the group status can be reachable)
Configure the scheduling interval between the members in the RTR entity group	**interval** *interval*	Optional By default, the scheduling interval of the members in the group is 0s.
Configure the RTR entity group to generate the scheduler automatically	**group probe**	Optional By default, do not configure the RTR entity group to generate the scheduler automatically.

NOTE

- One VoIP-jitter entity or UDP-echo entity cannot be added to multiple groups for scheduling. Otherwise, the scheduling result may be wrong.
- The calculation method for the scheduling interval of the RTR entity group is as follows: scheduling interval = the maximum of all member scheduling intervals + (member quantity

– 1) * scheduling interval between the members.

74.2.4 Configure RTR Responder -S -E -A

The RTR responder is mainly used to set up the connection with the source end and respond the detection packets sent by the source end, so as to ensure that the detection result is correct. The VoIP-jitter entity and the UDP-echo entity need to set up the connection with the destination end, so we should configure the RTR responder at the destination end.

Configuration Conditions

Before configuring the RTR responder, first complete the following task:

- Enable RTR.

Configure RTR Responder

Table 74-13 Configure the RTR Responder

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the RTR responder	**rtr responder**	Mandatory

74.2.5 Configure RTR Scheduler -S -E -A

The RTR scheduler is the policy of the scheduling detection for the RTR entity or group. The RTR scheduler can take one entity member as the object and also can take one RTR entity group as the object, but cannot take the group and entity as the object together. The RTR scheduler is identified by the schedule ID uniquely and not related with the RTR entity type, but the scheduling interval should consider the attributes of the scheduled RTR entity or the members in the RTR entity group. The RTR scheduler provides rich scheduling policies and can select to schedule at once or start to schedule after some time, even can set the absolute time of starting the scheduling. Besides, the scheduler can automatically demise after the set scheduling times and also can always exist.

Configuration Conditions

Before configuring the RTR scheduler, first complete the following task:

- Configure the desired RTR entity or RTR entity group

Configure RTR Scheduler

Table 74-14 Configure the RTR Scheduler

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the RTR scheduler, scheduling one entity or group	**rtr schedule** *schedule-id* { **entity** *entity-id* | **group** *group-id* } **start** { *hh:mm* [:*ss*] *date month year* | **after** *hh:mm* [:*ss*] | **now** } **ageout** *ageout-time* **life** { **forever** | *life-time* **repeat** *repeat-times* }	Mandatory

NOTE

- The age time of the RTR scheduler should be larger than the scheduling interval of the scheduling object. Otherwise, after one scheduling, the scheduler is deleted because of aging and timeout.

74.2.6 Configure Pausing Scheduling Entity *-S -E -A*

For the entity being scheduled, we can configure pausing scheduling the entity.

Configuration Conditions

Before configuring pausing scheduling the entity, first complete the following task:

- The entity is being scheduled

Configure Pausing Scheduling Entity

Table 74-15 Configure Pausing Scheduling the Entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure pausing scheduling the entity	**rtr** *entity-id* **halt**	Optional

NOTE

- Only one entity can configure **rtr halt**. If the entity is the member of the RTR entity group, we cannot configure **rtr halt.**

- After configuring **rtr halt** and if still not configuring **rtr resume** before the scheduling period ends, the scheduler of scheduling the entity is deleted because of aging and timeout.

74.2.7 Configure Restoring Scheduling Entity *-S -E -A*

For the entity paused scheduling, we can configure restoring scheduling the entity.

Configuration Conditions

Before configuring restoring scheduling the entity, first complete the following task:

- The entity is in the paused scheduling state

Configure Restoring Scheduling Entity

Table 74-16 Configure Restoring Scheduling the Entity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure restoring scheduling the entity	**rtr** *entity-id* **resume**	Optional

74.2.8 SLA Monitoring and Maintaining *-S -E -A*

Table 74-17 SLA Monitoring and Maintaining

Command	Description
show rtr entity [*entity-id*]	Display the RTR entity information
show rtr group [*group-id*]	Display the information of the RTR entity group
show rtr history *entity-id*	Display the history record information of the specified RTR entity
show rtr schedule [*schedule-id*]	Display the information of the RTR scheduler

74.3 SLA Typical Configuration Example

74.3.1 Configure ICMP-echo Entity to Detect Basic Network Communication *-S -E* *-A*

Network Requirements

- Use the ICMP-echo entity on Device1, detecting the basic communication of the network from Device1 to Device3.

Network Topology

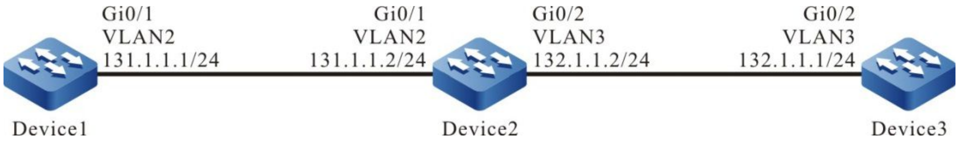


Figure 74–1 Networking of Configuring ICMP-echo Entity

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address and route of the interface, making Device1 communicate with Device3. (Omitted)

Step 3: Configure the ICMP-echo entity and add the attribute parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpecho
Device1(config-rtr-icmpecho)#set 132.1.1.1 5 70 2 12 extend 131.1.1.1 0 TRUE FALSE
Device1(config-rtr-icmpecho)#alarm-type log
Device1(config-rtr-icmpecho)#number-of-history-kept 255
Device1(config-rtr-icmpecho)#threshold-pktLoss 10 direction be
Device1(config-rtr-icmpecho)#threshold-rtt 1000  direction be
Device1(config-rtr-icmpecho)#exit
```

#View the ICMP-echo entity parameters.

```
Device1#show rtr entity 1
----------------------------------------------------------------
ID:1          name:IcmpEcho1        Created:TRUE
****************type:ICMPECHO****************
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:0
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:0
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
```

```
Periods:1
Extend parameters:
sourceIp:131.1.1.1      tos:0   DF(DON'T FRAG):TRUE     Verify-data:FALSE
In-scheduling:FALSE
Schedule frequency:12(s)
Status:DEFAULT
```

The result shows that the entity parameters are consistent with the configuration.

In-scheduling:FALSEDescription entity is not scheduled.

Status:DEFAULTDescription entity status is DEFAULT.

NOTE

- When the entity is not scheduled, the status is DEFAULT; when the entity is scheduled and if the entity is reachable, the status is REACHABLE; if the entity is unreachable, the status is UNREACHABLE.

Step 4: Schedule the defined ICMP-echo entity and define the attribute parameters of the scheduling.

#Configure Device1

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

Step 5: Check the result.

(1) When the network connectivity from Device1 to Device3 is normal:

#View the entity status.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1            name:IcmpEcho1          Created:TRUE
****************type:ICMPECHO****************
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:1
Time-of-last-schedule:WED OCT 31 14:54:07 2012
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:5
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1      tos:0   DF(DON'T FRAG):TRUE     Verify-data:FALSE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:REACHABLE
```

In-scheduling: TRUE indicates that the entity is being scheduled;

Status:REACHABLE indicates that the entity status is reachable, that is, the network connection from Device1to Device3 is normal.

(2) When the network connectivity from Device1 to Device3 is faulty:

The alarm mode is configured as log, so when the network is disconnected, print the alarm information on the device, as follows:

```
Oct 31 14:54:46: [tRtrIcmpRcv]Rtr 1 (ICMPECHO) rtt [9000ms] was exceeded(>=) threshold [1000ms].
```

#View the entity status.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1          name:IcmpEcho1         Created:TRUE
****************type:ICMPECHO****************
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:4
Time-of-last-schedule:WED OCT 31 14:54:43 2012
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:20
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1      tos:0   DF(DON'T FRAG):TRUE     Verify-data:FALSE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:UNREACHABLE
```

In-scheduling: TRUED indicates that the entity is being scheduled;

Status:UNREACHABLE indicates that the entity status is unreachable, that is, the network connection from Device1to Device3 is unreachable.

#View the history record content.

```
Device1#show rtr history 1
---------------------------------------------------------------
ID:1    Name:IcmpEcho1  CurHistorySize:4        MaxHistorysize:255
History recorded as following:
WED OCT 31 14:54:46 2012
       PktLoss:5         ,Rtt:invalid
WED OCT 31 14:54:32 2012
       PktLoss:0         ,Rtt:11        (ms)
WED OCT 31 14:54:20 2012
       PktLoss:0         ,Rtt:2         (ms)
WED OCT 31 14:54:07 2012
       PktLoss:0         ,Rtt:2         (ms)
```

In the history records, record the packet loss and delay of each scheduling; if Rtt is invalid, it indicates that there is fault in the network and the network is reachable.

74.3.2 Configure ICMP-path-echo Entity to Detect Network Communication

-S -E -A

Network Requirements

- Use the ICMP-path-echo entity on Device1, detecting the path network communication from Device1 to Device3.

Network Topology

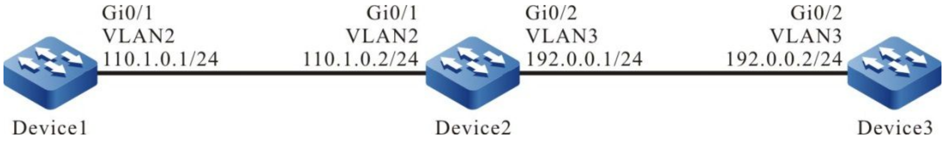


Figure 74–2 Networking of Configuring the ICMP-path-echo Entity

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address and route of the interface, making Device1, Device2, and Device3 communicate with each other. (Omitted)

Step 3: Configure the ICMP-path-echo entity and add the attribute parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmp-path-echo
Device1(config-rtr-icmppathecho)#set dest-ipaddr 192.0.0.2 source-ipaddr 110.1.0.1
Device1(config-rtr-icmppathecho)#number-of-history-kept 255
Device1(config-rtr-icmppathecho)#targetOnly false
Device1(config-rtr-icmppathecho)#exit
```

#View the ICMP-path-echo entity parameters.

```
#View the ICMP-path-echo entity parameters.
Device1#show rtr entity 1
------------------------------------------------------------------
ID:1          name:IcmpPathEcho1          Created:TRUE
****************type:ICMPPATHECHO****************
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:0
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
------------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration.

In-scheduling:FALSE indicates that the entity is not scheduled.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 4: Schedule the defined ICMP-path-echo entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step 5: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
----------------------------------------------------------------
ID:1           name:IcmpPathEcho1              Created:TRUE
****************type:ICMPPATHECHO****************
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:1
Time-of-last-schedule:WED OCT 24 10:20:01 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:TRUE
Status:REACHABLE
```

In-scheduling:TRUE indicates that the entity is being scheduled.

Status:REACHABLE indicates that the entity status is reachable, that is, the network connection from Device1to Device3 is normal.

#View the history record content.

```
Device1#show rtr history 1
----------------------------------------------------------------
ID:1    Name:IcmpPathEcho1
History of hop-by-hop:
 110.1.0.2      PktLoss:0       ,Rtt:2         (ms)
 192.0.0.2      PktLoss:0       ,Rtt:1         (ms)
History of record from source to dest:
CurHistorySize:1        MaxHistorysize:255
WED OCT 24 10:20:01 2012
       PktLoss:0       ,Rtt:1         (ms)
```

In the history records, record the packet loss and delay of each scheduling.

#Wait for some time and after scheduling for 10 times, view the entity status.

```
Device1#show rtr entity 1
----------------------------------------------------------------
ID:1           name:IcmpPathEcho1              Created:TRUE
****************type:ICMPPATHECHO****************
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:10
Time-of-last-schedule:WED OCT 24 10:29:01 2012
```

```
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
```

After scheduling for 10 times, the scheduling stops and the entity status is DEFAULT.

74.3.3 Configure ICMP-path-jitter Entity to Detect Network Communication

-S -E -A

Network Requirements

- Use the ICMP-path-jitter entity on Device1, detecting the path network communication from Device1 to Device3.

Network Topology

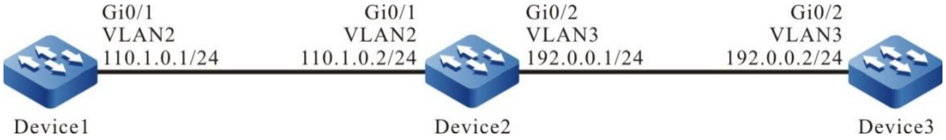


Figure 74–3 Networking of Configuring the ICMP-path-jitter Entity

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address and route of the interface, making Device1, Device2, and Device3 communicate with each other. (Omitted)

Step 3: Configure the ICMP-path-jitter entity and add the attribute parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmp-path-jitter
Device1(config-rtr-icmppathjitter)#set dest-ipaddr 192.0.0.2 10 20 source-ipaddr 110.1.0.1
Device1(config-rtr-icmppathjitter)#number-of-history-kept 255
Device1(config-rtr-icmppathjitter)#targetOnly false
Device1(config-rtr-icmppathjitter)#exit
```

#View the ICMP-path-jitter entity parameters.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1          name:IcmpPathJitter1          Created:TRUE
****************type:ICMPPATHJITTER****************
CreatedTime:WED OCT 24 10:54:31 2012
```

```
LatestModifiedTime:WED OCT 24 10:56:12 2012
Times-of-schedule:0
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:10 (each hop)
Packets-interval:20(ms)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktLoss: 200000000  direction:be
Threshold-of-jitter:6000(ms) direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
---------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration.

In-scheduling:FALSE indicates that the entity is not scheduled.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 4: Schedule the defined ICMP-path-jitter entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life foreve
```

Step 5: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1          name:IcmpPathJitter1          Created:TRUE
*****************type:ICMPPATHJITTER****************
CreatedTime:WED OCT 24 10:54:31 2012
LatestModifiedTime:WED OCT 24 10:56:12 2012
Times-of-schedule:4
Time-of-last-schedule:WED OCT 24 11:00:25 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:10 (each hop)
Packets-interval:20(ms)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktLoss: 200000000 direction:be
Threshold-of-jitter:6000(ms) direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:TRUE
Status:REACHABLE
---------------------------------------------------------------
```

In-scheduling: TRUE indicates that the entity is being scheduled.

Status:REACHABLE indicates that the entity status is reachable, that is, the network connection from Device1to Device3 is normal.

#View the history record content.

```
Device1#show rtr history 1
------------------------------------------------------------
ID:1    Name:IcmpPathJitter1
History of hop-by-hop:
 110.1.0.2      PktLoss:0        Rtt:1        (ms),Jitter:0        (ms)
 192.0.0.2      PktLoss:0        Rtt:0        (ms),Jitter:0        (ms)
History of record from source to dest:
CurHistorySize:4       MaxHistorysize:255
WED OCT 24 11:00:25 2012
       PktLoss:0        ,Rtt:1       (ms),Jitter:0        (ms)
WED OCT 24 10:59:25 2012
       PktLoss:0        ,Rtt:0       (ms),Jitter:0        (ms)
WED OCT 24 10:58:25 2012
       PktLoss:0        ,Rtt:0       (ms),Jitter:0        (ms)
WED OCT 24 10:57:25 2012
       PktLoss:0        ,Rtt:0       (ms),Jitter:0        (ms)
------------------------------------------------------------
```

In the history records, record the packet loss, delay and jitter of each scheduling.

74.3.4 Configure VoIP-jitter Entity to Detect Network Transmitting VoIP Packets

-S -E -A

Network Requirements

- Use the VoIP-jitter entity on Device1 and detect the network transmitting VoIP packets from Device1 to Device3.

Network Topology

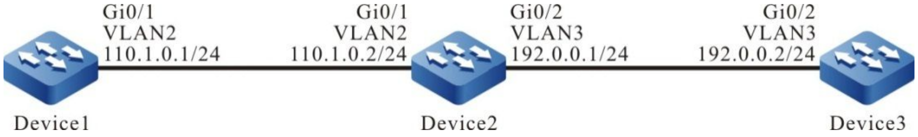


Figure 74–4 Networking of Configuring the VoIP-jitter Entity

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address and route of the interface, making Device1 communicate with Device3. (Omitted)

Step 3: Configure ntp and synchronize the clock.

#Configure Device3.

```
Device3#config terminal
Device3(config)#ntp master
```

#Configure Device1.

```
Device1(config)#ntp server 192.0.0.2
```

#View that Device3 becomes the clock server successfully and prompt that the clock is synchronized.

```
Device3#show ntp status
Current NTP status information
Clock is synchronized, stratum 8, reference is 127.127.8.10
reference time is D4321EF4.7BBBBB68 (08:01:56.483 Wed Oct 24 2012)
```

#View that Device1 becomes the clock client successfully, prompt that the clock is synchronized and display the server address.

```
Device1#show ntp status
Current NTP status information
Clock is synchronized, stratum 9, reference is 192.0.0.2
reference time is D43222C1.91110F31 (08:18:09.566 Wed Oct 24 2012)
```

Step 4: Configure responder on Device3 as the responder end.

#Configure Device3

```
Device3(config)#rtr enable
Device3(config)#rtr responder
```

Step 5: Configure the VoIP-jitter entity on Device1 and add the attribute parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 jitter
Device1(config-rtr-jitter)#set dest-ipaddr 192.0.0.2 dest-port 1234 g711alaw source-ipaddr 110.1.0.1 source-port 1234
Device1(config-rtr-jitter)#number-of-history-kept 255
Device1(config-rtr-jitter)#exit
```

#View the entity parameter.

```
Device1#show rtr entity 1
-------------------------------------------------------------
ID:1          name:Jitter1          Created:TRUE
****************type:JITTER****************
CreatedTime:WED OCT 24 16:02:32 2012
LatestModifiedTime:WED OCT 24 16:02:58 2012
Times-of-schedule:0
Entry-state:Pend
TargetIp:192.0.0.2      targetPort:1234
Codec:G.711 A-Law       Packet-size:172 Packet-number:1000
Packet-transmit-interval:20(ms)
frequency:60(s)
SourceIp:110.1.0.1      Soure-port:1234
TimeOut:50000(ms)
Alarm-type:none
Threshold-of-dsDelay:5000(ms) direction:be
Threshold-of-dsJitter:6000(ms) direction:be
Threshold-of-dsPktLoss:200000000 direction:be
Threshold-of-sdDelay:5000(ms) direction:be
Threshold-of-sdJitter:6000(ms) direction:be
Threshold-of-sdPktLoss:200000000 direction:be
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-mos:10000000 direction:be
Threshold-of-icpif:100000000 direction:be
Number-of-history-kept:255
Periods:1
Status:DEFAULT
-------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 6: Schedule the defined VoIP-jitter entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step7: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1          name:Jitter1          Created:TRUE
****************type:JITTER****************
CreatedTime:WED OCT 24 16:02:32 2012
LatestModifiedTime:WED OCT 24 16:06:02 2012
Times-of-schedule:3
Time-of-last-schedule:WED OCT 24 16:08:29 2012
Entry-state:Transmit
TargetIp:192.0.0.2      targetPort:1234
Codec:G.711 A-Law       Packet-size:172 Packet-number:1000
Packet-transmit-interval:20(ms)
frequency:60(s)
SourceIp:110.1.0.1      Soure-port:1234
TimeOut:50000(ms)
Alarm-type:none
Threshold-of-dsDelay:5000(ms) direction:be
Threshold-of-dsJitter:6000(ms) direction:be
Threshold-of-dsPktLoss:200000000 direction:be
Threshold-of-sdDelay:5000(ms) direction:be
Threshold-of-sdJitter:6000(ms) direction:be
Threshold-of-sdPktLoss:200000000 direction:be
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-mos:10000000 direction:be
Threshold-of-icpif:100000000 direction:be
Number-of-history-kept:255
Periods:1
Status:REACHABLE
---------------------------------------------------------------
```

Entry-state:Transmit indicates that the entity is being scheduled.

Status:REACHABLE indicates that the entity status is reachable and the network from Device1 to Device3 transmits the VoIP packets normally.

#View the history record contents.

```
Device1#show rtr history 1
---------------------------------------------------------------
ID:1    Name:Jitter1    CurHistorySize:3       MaxHistorysize:255
History recorded as following:
WED OCT 24 16:08:46 2012
      SdPktLoss:0          ,DsPktLoss:0          ,Rtt:185      (ms),
      SdDelay:14      (ms),DsDelay:178      (ms),SdJitter:8       (ms),DsJitter:183      (ms),
      Mos:5.000000         ,icpif:0.000000
WED OCT 24 16:07:45 2012
      SdPktLoss:0          ,DsPktLoss:0          ,Rtt:14       (ms),
      SdDelay:16      (ms),DsDelay:7       (ms),SdJitter:10      (ms),DsJitter:13       (ms),
      Mos:5.000000         ,icpif:0.000000
WED OCT 24 16:06:46 2012
```

```
    SdPktLoss:0          ,DsPktLoss:0          ,Rtt:17       (ms),
    SdDelay:16       (ms),DsDelay:9       (ms),SdJitter:11       (ms),DsJitter:13       (ms),
    Mos:5.000000          ,icpif:0.000000
-------------------------------------------------------------
```

In the history records, record the uni-directional packet loss, turnaround delay, uni-directional delay, and uni-directional jitter of each scheduling.

NOTE

- Before configuring the VoIP-jitter entity, we need to configure the NTP service to realize the network clock synchronization and configure the **rtr responder** command at the destination end as the responder. Note that if the clock is not synchronized or not configuring the responder end, the scheduling result is wrong.

74.3.5 Configure UDP-echo Entity to Detect Network Transmitting UDP Packets

-S -E -A

Network Requirements

- Use the UDP-echo entity on Device1 and detect the network transmitting UDP packets from Device1 to Device3.

Network Topology

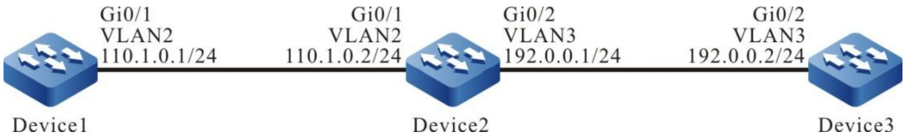


Figure 74–5 Networking of Configuring the UDP-echo Entity

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address and route of the interface, making Device1 communicate with Device3. (Omitted)

Step 3: Configure responder on Device3 as the responder end.

#Configure Device3

```
Device3#config terminal
Device3(config)#rtr enable
Device3(config)#rtr responder
```

Step 4: Configure the UDP-echoentity on Device1 and add the attribute parameters.

#Configure Device1.

```
Device1#config terminal
```

```
Device1(config)#rtr enable
Device1(config)#rtr 1 udpecho
Device1(config-rtr-udpecho)#set dest-ipaddr 192.0.0.2 dest-port 1001 source-ipaddr 110.1.0.1 source-port
1001
Device1(config-rtr-udpecho)#number-of-history-kept 255
Device1(config-rtr-udpecho)#frequency 10
Device1(config-rtr-udpecho)#exit
```

#View the entity parameter.

```
Device1#show rtr entity 1
--------------------------------------------------------------
ID:1          name:UdpEcho1          Created:TRUE
****************type:UDPECHO****************
CreatedTime:WED OCT 24 16:36:45 2012
LatestModifiedTime:WED OCT 24 16:37:44 2012
Times-of-schedule:0
Entry-state:Pend
TargetIp:192.0.0.2      TargetPort:1001
SourceIp:110.1.0.1      SourePort:1001
TimeOut:5000(ms)
request-data-size:16
Frequecy:10(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
Status:DEFAULT
--------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 5: Schedule the defined UDP-echo entity and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

Step 6: Check the result.

#View the entity status.

```
Device1#show rtr entity 1
--------------------------------------------------------------
ID:1          name:UdpEcho1          Created:TRUE
****************type:UDPECHO****************
CreatedTime:WED OCT 24 16:36:45 2012
LatestModifiedTime:WED OCT 24 16:37:44 2012
Times-of-schedule:5
Time-of-last-schedule:WED OCT 24 16:39:50 2012
Entry-state:Pend
TargetIp:192.0.0.2      TargetPort:1001
SourceIp:110.1.0.1      SourePort:1001
TimeOut:5000(ms)
request-data-size:16
Frequecy:10(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Data-pattern:ABCD
Number-of-history-kept:255
Periods:1
Status:REACHABLE
```

```
----------------------------------------------------------------
```

Status:REACHABLE indicates that the entity status is reachable, that is, the network from Device1 to Device2 can transmits the UDP packets normally.

#View the history record content.

```
Device1#show rtr history 1
----------------------------------------------------------------
ID:1    Name:UdpEcho1   CurHistorySize:5      MaxHistorysize:255
History recorded as following:
WED OCT 24 16:39:54 2012
       PktLoss:0       ,Rtt:1        (ms)
WED OCT 24 16:39:44 2012
       PktLoss:0       ,Rtt:1        (ms)
WED OCT 24 16:39:33 2012
       PktLoss:0       ,Rtt:2        (ms)
WED OCT 24 16:39:23 2012
       PktLoss:0       ,Rtt:2        (ms)
WED OCT 24 16:39:13 2012
       PktLoss:0       ,Rtt:2        (ms)
----------------------------------------------------------------
```

In the history records, record the packet loss and delay of each scheduling.

NOTE

- Before configuring the UDP-echo entity, we need to configure the rtr responder command at the destination end as the responder. If the responder end is not configured, the scheduling result is wrong.

74.3.6 Configure FLOW-statistics Entity to Detect Interface Traffic *-S -E -A*

Network Requirements

- On Device1, use FLOW-statistics entity to detect the traffic of interface vlan2.

Network Topology

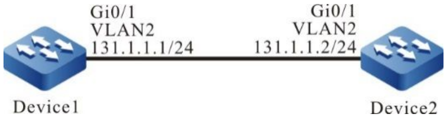


Figure 74-6 Configure FLOW-statistics Entity Networking

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: On Device1, configure the FLOW-statistics entity and add property parameters.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 flow-statistics
Device1(config-rtr-flowsta)#flow-statistics interface vlan 2 interval 60
Device1(config-rtr-flowsta)#number-of-history-kept 255
Device1(config-rtr-flowsta)#exit
```

#View entity parameters.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1         name:flow-statistics1         Created:TRUE
****************type:FLOWSTATISTICS****************
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:0
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface: vlan2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:DEFAULT
---------------------------------------------------------------
```

The results show that the entity parameters are consistent with the configuration.

Status: DEFAULT indicates that the entity status is DEFAULT.

Step 3: Call the FLOW-statistics entity defined to define the property parameters scheduled.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

Step 4: Check the result.

1) When there is received data traffic on the interface vlan2:

#View entity status.

```
Device1#show rtr entity 1
---------------------------------------------------------------
ID:1         name:flow-statistics1         Created:TRUE
```

```
****************type:FLOWSTATISTICS****************
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:2
Time-of-last-schedule:THU OCT 25 10:02:11 2012
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface: vlan 2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:REACHABLE
--------------------------------------------------------------
```

Status: REACHABLE indicates that the entity status is reachable, i.e. there is a datagram in / out the interface vlan2.

2) When there is no data traffic in / out the interface vlan2:

#View entity status.

```
Device1#show rtr entity 1
--------------------------------------------------------------
ID:1          name:flow-statistics1          Created:TRUE
****************type:FLOWSTATISTICS****************
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:5
Time-of-last-schedule:THU OCT 25 10:05:11 2012
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface: vlan 2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:UNREACHABLE
--------------------------------------------------------------
```

Status: UNREACHABLE indicates that when there is no traffic in / out the interface vlan2, the entity status is unreachable.

#View the history.

```
Device1#show rtr history 1
---------------------------------------------------------------
ID:1          Name:flow-statistics1   CurHistorySize:5      MaxHistorysize:255
History recorded as following:
THU OCT 25 10:05:11 2012
       Input pkt:0          (packets/s),Input flow:0         (bits/s),
       Output pkt:0         (packets/s),Output flow:0        (bits/s)
THU OCT 25 10:04:11 2012
       Input pkt:209        (packets/s),Input flow:214000   (bits/s),
       Output pkt:0         (packets/s),Output flow:0        (bits/s)
THU OCT 25 10:03:11 2012
       Input pkt:8460       (packets/s),Input flow:8663000   (bits/s),
       Output pkt:0         (packets/s),Output flow:0        (bits/s)
THU OCT 25 10:02:11 2012
       Input pkt:8460       (packets/s),Input flow:8663000   (bits/s),
       Output pkt:0         (packets/s),Output flow:0        (bits/s)
THU OCT 25 10:01:12 2012
       Input pkt:6456       (packets/s),Input flow:6610000   (bits/s),
       Output pkt:0         (packets/s),Output flow:0        (bits/s)
---------------------------------------------------------------
```

The history details the rate of each schedule in/out of the interface vlan2 (based on amount and bit).

NOTE

- FLOW-statistics entity REACHEABLE: when the entity is in scheduling, the entity is REACHEABLE in state as long as there is traffic in the interface IN or OUT direction, or UNREACHABLE if there is no traffic.

74.3.7 Configure TRACK to Link with SLA *-S -E -A*

Network Requirements

- TRACK links with SLA. Judge the validity of the static route on Device1 via the entity status.

Network Topology

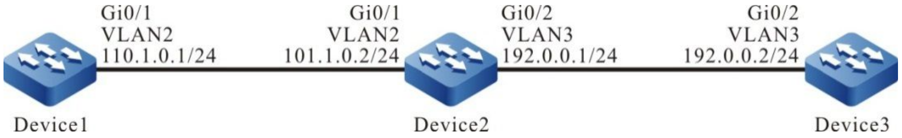


Figure 74–7 Networking of Configuring TRACK to Link with SLA

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the ICMP-echo entity on Device1 to detect the network connectivity from Device1 to Device2, and add the entity to the entity group.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpecho
Device1(config-rtr-icmpecho)#set 110.1.0.2 5 70 2 12 extend 110.1.0.1 0 true false
Device1(config-rtr-icmpecho)#number-of-history-kept 255
Device1(config-rtr-icmpecho)#exit
Device1(config)#rtr group 1
Device1(config-rtr-group)#member 1
Device1(config-rtr-group)#exit
```

Step 4: Define TRACK and associate with LSA.

#Configure Device1.

```
Device1(config)#track 1
Device1(config-track)#rtr 1
```

Step 5: Add the static route and associate TRACK.

#Configure Device1.

```
Device1(config)#ip route 192.0.0.0 255.255.255.0 110.1.0.2 track 1
```

Step 6: Schedule the entity and check the validity of the static route.

#Configure Device1.

```
Device1(config)#rtr schedule 1 group 1 start now ageout 100 life forever
```

Step 7: Check the result.

(1) When the network connectivity from Device1 to Device2 is normal:

#View the entity group status.

```
Device1#show rtr group 1
----------------------------------------------
ID:1           name:rtrGroup1         Members schedule interval:0
Option: AND     Status:REACHABLE
*****************************
type:SINGLE     Entity Id :1
```

The status of the entity group is REACHEABLE.

#In the route table of Device1, view the route of the segment 192.0.0.0/24.

```
Device1#show ip route 192.0.0.0
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

S   192.0.0.0/24 [1/10] via 110.1.0.2, 00:00:09, gigabitethernet0/1
```

The result displays that there is the route to the segment 192.0.0.0/24, indicates that when the status of the entity group is RECHABLE, judge that the static route is valid.

(2) When the network connectivity from Device1 to Device2 is faulty:

#View the status of the entity group:

```
Device1#show rtr group 1
----------------------------------------------
ID:1           name:rtrGroup1         Members schedule interval:0
Option: AND     Status:UNREACHABLE
*****************************
type:SINGLE     Entity Id :1
```

The status of the entity group is UNREACHEABLE.

#In the route table of Device1, view the route of the segment 192.0.0.0/24.

```
Device1#show ip route 192.0.0.2
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

The result displays that there is no route to the segment 192.0.0.0/24, indicates that when the status of the entity group is UNREACHABLE, judge that the static route is invalid.

75 NTP

75.1 Overview

NTP (Network Time Protocol) is the standard Internet protocol used to synchronize the time in Internet. NTP is to synchronize the device time to the standard time. Currently, the adopted time standard is UTC (Universal Time Coordinated).

The design of NTP fully considers the complexity of the time synchronization on Internet. NTP provides the strict, practical, and valid mechanism, applicable to the Internet environments with various scales and speeds. NTP not only corrects the present time, but also continuously tracks the time change and can adjust automatically. Even if the network fails, it can maintain the time stability. The network cost generated by NTP is small and has the measures of ensuring the network security. The measures can make NTP get the reliable and correct time synchronization on Internet.

75.2 NTP Function Configuration

Table 75-1 NTP Function Configuration List

Configuration Task	
Configure the NTP basic functions	Enable the NTP server
	Enable the NTP client
Configure the NTP optional parameters	Configure the NTP source interface
Configure the NTP authentication functions	Configure the NTP client authentication
	Configure the NTP server authentication
Configure the NTP access control	Configure the NTP access control

75.2.1 Configure NTP Basic Functions *-B -S -E -A*

Configuration Conditions

Before configuring the NTP basic functions, first complete the following task:

- Configure the network layer address of the interface, making the NTP client/server network layer reachable.

Enable NTP Server

When the device needs to provide the time service for other devices, we can configure the local device as the NTP server and adopt the local time as the clock source.

Table 75-2 Enable the NTP Server

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the NTP server	**ntp master** [*stratum-number*]	Mandatory By default, do not enable the NTP server function.

Enable NTP Client

When there is the NTP server in the network and if the device needs to synchronize the time from the NTP server, we need to enable the NTP client function at the local device, specify the IP address of the server and select configuring the NTP protocol version, authentication key and the source interface of the NTP packet.

Table 75-3 Enable the NTP Client

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the NTP client	**ntp server** [**vrf** *vrf-name*] { *ip-address* | *domain-name* } [**version** *version*] [**key** *key-number*] **source** *interface-name*	Mandatory By default, do not enable the NTP client.

NOTE

- The *ip-address* parameter is one unicast address, but cannot be the broadcast address, multicast address or local device IP address.
- After specifying the source interface of the NTP packet via **source** *interface-name*, the master IP address of the interface is set as the source IP address of the NTP packet.

75.2.2 Configure NTP Optional Parameters *-B -S -E -A*

Configuration Conditions

None

Configure NTP Source Interface

NTP supports configuring the source interface of sending the packet. When it is necessary to send the NTP packet, select the master address of the source interface as the source IP address of the packet. The packet is sent out from the specified interface.

Table 75-4 Configure the NTP Source Interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the NTP source interface	**ntp source** *interface-name*	Optional By default, do not configure the NTP source interface.

NOTE

- If we use the **ntp server** command to specify the source interface, first use the **ntp server** command to specify the source interface.

75.2.3 Configure NTP Authentication Function *-B -S -E -A*

Configuration Conditions

None

Configure NTP Client Authentication

To ensure the communication security between the NTP client and the server, we can perform the MD5 authentication for the packet received by the client, ensuring that the client is synchronized with the valid time.

Table 75-5 Configure the NTP Client Authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enable the authentication function of the NTP client	**ntp authenticate**	Mandatory By default, NTP disables the authentication function.
Configure the authentication key	**ntp authentication-key** *key-number* **md5** *key*	Mandatory By default, do not configure the authentication key.
Configure the trusted key	**ntp trusted-key** *key-number*	Mandatory By default, do not configure the trusted key.
Specify the associated key	**ntp server** [**vrf** *vrf-name*] *ip-address* | *domain-name* [**version** *version*] [**key** *key-number*] [**source** *interface-name*]	Mandatory

NOTE

- The NTP server and client need to be configured with the same authentication key.

Configure NTP Server Authentication

To support the authentication with the NTP client, the NTP server needs to be configured with the same authentication key as the client.

Table 75-6 Configure the NTP Server Authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the authentication key	**ntp authentication-key** *key-number* **md5** *key*	Mandatory By default, the server is not configured with

Step	Command	Description
		the authentication key.

75.2.4 Configure NTP Access Control *-B -S -E -A*

Configuration Conditions

To configure the NTP access control, first complete the following task:

- Configure the ACL associated with the access control

Configure NTP Access Control

NTP can limit the access for the local NTP server by associating with ACL.

Table 75-7 Configure the NTP Access Control

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the NTP access control	**ntp access-group peer** *access-list-number*	Mandatory By default, do not configure the access control.

75.2.5 NTP Monitoring and Maintaining *-B -S -E -A*

Table 75-8 NTP Monitoring and Maintaining

Command	Description
show ntp status	Display the NTP status information

75.3 NTP Typical Configuration Example

75.3.1 Configure NTP Server and Client *-B -S -E -A*

Network Requirements

- Device1 is the NTP server and Device2 is the NTP client.

- Device1 and Device2 are interconnected via their interfaces and the route is reachable.
- The NTP server is the clock source and the client gets the clock from the server.

Network Topology

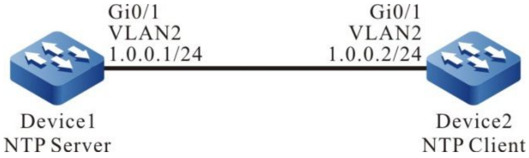


Figure 75-1 Networking of Configuring NTP Server and Client

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the NTP server Device1.

#Configure the local clock of the device as the reference clock the clock layers are 3.

```
Device1#configure terminal
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 4: Configure the NTP client Device2.

#Configure Device2 as the Beijing time zone.

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING +8
```

#Specify the NTP server Device1 and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
Device2(config)#exit
```

Step 5: Check the result.

#Execute the **show ntp status** command on the client Device2, and view the clock synchronization status, indicating that the client and NTP server Device1 are synchronized and the clock layers is 4, larger than Device1.

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442EB0E.432F29BD (01:49:02.262 Tue Nov 06 2012)
```

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock

BEIJING(UTC+08:00) TUE NOV 06 09:49:30 2012
```

75.3.2 Configure NTP Server and Multi-level Clients *-B -S -E -A*

Network Requirements

- Device1 is the NTP server; Device2 and Device3 are the NTP clients.
- Device2 are interconnected with Device1 and Device 3; the route is reachable.
- Device1 provides the clock for Device2; Device2 provides the clock for Device3.

Network Topology

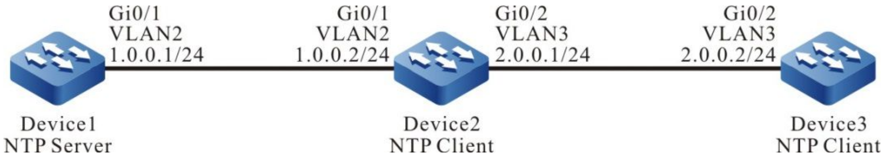


Figure 75-2 Networking of Configuring the NTP Server and Multi-level Clients

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the NTP server Device1.

#Configure the local clock of the device as the reference clock and the clock layers is 3.

```
Device1#configure terminal
Device1(config)#ntp master 3
```

Step 4: Configure the NTP client Device2.

#Configure Device2 as Beijing time zone.

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING +8
```

#Specify the NTP server Device2 and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
```

Step 5: Configure the NTP client Device3.

#Configure Device3 as Beijing time zone.

```
Device3#configure terminal
Device3(config)#clock timezone BEIJING +8
```

#Specify the NTP server Device2 and the IP address is 2.0.0.1.

```
Device3(config)#ntp server 2.0.0.1
```

Step 6: Check the result, viewing the clock synchronization information on Device2 and Device3.

#Execute the **show ntp status** command on the client Device2, and view the clock synchronization status, indicating that Device2 and NTP server Device1 are synchronized and the clock layers is 4, larger than Device1.

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D44CC35E.BAA6A190 (13:02:22.729 Tue Nov 13 2012)
```

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock

BEIJING(UTC+08:00) TUE NOV 13 21:02:24 2012
```

#Execute the **show ntp status** command on the client Device3, and view the clock synchronization status, indicating that Device3 and Device2 are synchronized and the clock layers is 5, larger than Device1.

```
Device3#show ntp status
Current NTP status information
Clock is synchronized, stratum 5, reference is 2.0.0.1
reference time is D44CC365.5CC8C4C8 (13:02:29.362 Tue Nov 13 2012)
```

#Execute the **show clock** command to view the device clock on the client Device3.

```
Device3#show clock

BEIJING(UTC+08:00) TUE NOV 13 21:02:36 2012
```

75.3.3 Configure NTP Server and Client with MD5 Authentication *-B -S -E -A*

Network Requirements

- Device1 is the NTP server; Device2 is the NTP client; both adopt the MD5 algorithm authentication.
- Device1 and Device2 are interconnected via their interfaces; the route is reachable.
- NTP server is the clock source and the client gets the clock from the server.

Network Topology

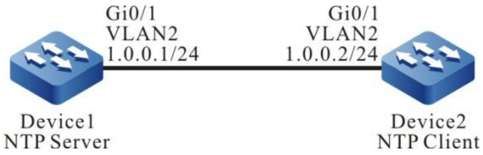


Figure 75-3 Networking of Configuring the NTP Server and Client with MD5 Authentication

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the NTP server.

#Configure the local clock of the device as the reference clock and the clock layers is 3.

```
Device1#configure terminal
Device1(config)#ntp master 3
```

#Enable the authentication.

```
Device1(config)#ntp authenticate
```

#Configure the authentication key serial number as 1, algorithm as MD5 and key as admin.

```
Device1(config)#ntp authentication-key 1 md5 admin
```

#Configure the key 1 be trusted.

```
Device1(config)#ntp trusted-key 1
```

Step 4: Configure the NTP client.

#Configure Device2 as Beijing time zone.

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING +8
```

#Specify the NTP server for the client and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1 key 1
```

#Enable the authentication.

```
Device2(config)#ntp authenticate
```

#Configure the authentication key serial number as 1, algorithm as MD5 and key as admin.

```
Device2(config)#ntp authentication-key 1 md5 admin
```

#Configure the key 1 be trusted.

```
Device2(config)#ntp trusted-key 1
```

Step 5: Check the result.

#Execute the **show ntp status** command on the client Device2, and view the clock synchronization status, indicating that the client and NTP server Device1 are synchronized and the clock layers is 4, larger than Device1.

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442ECE1.8BB7B219 (01:56:49.545 Tue Nov 06 2012)
```

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock

BEIJING(UTC+08:00) TUE NOV 06 09:56:52 2012
```

NOTE

- The authentication serial numbers of the NTP client and server should be the same and the keys should be the same.

75.3.4 Configure NTP Peer Mode *-B -S -E -A*

Network Requirements

- Device1, Device2 and Device3 are interconnected through their respective interfaces, and the route is reachable.
- Device1 sets the local clock as a reference with 3 layers.
- Device2 is NTP client and sets Device1 as NTP server.
- Device3 sets Device2 as peer. Device3 serves as active peer while Device2 serves as passive peer.

Network Topology

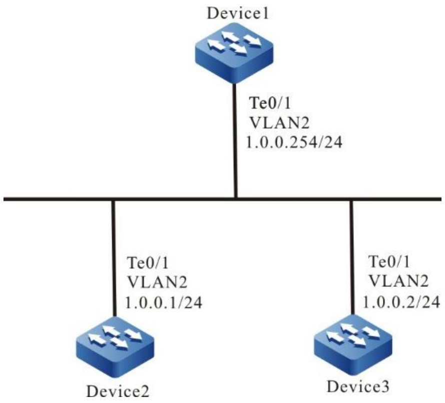


Figure 75-4 Configure NTP Peer Mode Networking

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Device1 sets the local clock as a reference with 3 layers.

```
Device1#configure terminal
Device1(config)#ntp master 3
```

Step 3: Device2 specifies Device1 as NTP server.

#Configure Device2 as Beijing time zone.

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING
```

#Specify the NTP server IP address as 1.0.0.254.

```
Device2(config)#ntp server 1.0.0.254
```

Step 4: Device3 sets Device2 as peer.

#Configure Device3 as Beijing time zone.

```
Device3#configure terminal
Device3(config)#clock timezone BEIJING
```

#Specify the NTP peer IP address as 1.0.0.1.

```
Device3(config)#ntp peer 1.0.0.1
```

Step 5: Check the result.

#On the client Device2, execute the **show ntp status** command to view the clock synchronization status and other information.

```
Device2#show ntp status

Current NTP status information

Clock is synchronized, stratum 4, reference is 1.0.0.254

reference time is D8E9785D.221F1F5 (03:09:17.8 Tue Apr 28 2015)
```

The number of clock layers of Device2 is 4, 1 more than that of Device1. The reference clock server address is 1.0.0.254, indicating that the client Device2 and the server Device1 have been synchronized.

#On the client Device2, execute the **show clock** command to view the Device clock.

```
Device2#show clock


BEIJING(UTC+08:00) TUE APR 28 11:10:36 2015
```

#On the active peer Device3, execute the **show ntp status** command to view the clock synchronization status and other information.

```
Device3#show ntp status

Current NTP status information

Clock is synchronized, stratum 5, reference is 1.0.0.1

reference time is D8E9795C.29835CC9 (03:13:32.162 Tue Apr 28 2015)
```

The number of clock layers of Device3 is 5, 1 more than that of Device2. The reference clock server address is 1.0.0.1, indicating that the active peer Device3 and the passive peer Device2 have been synchronized.

#On the client Device3, execute the **show clock** command to view the Device clock.

```
Device3#show clock


BEIJING(UTC+08:00) TUE APR 28 11:16:19 2015
```

75.3.5 Configure NTP Broadcasting Mode *-B -S -E -A*

Network Requirements

- Device1, Device2 and Device3 are interconnected through their respective interfaces, and the route is reachable.
- Device1 sets the local clock as a reference with 3 layers.
- Device1 is NTP broadcast server, and sends NTP broadcast packets from the interface VLAN2.
- Device2 and Device3 are NTP broadcast clients, and monitor NTP broadcast packets on their respective interface VLAN2.

Network Topology

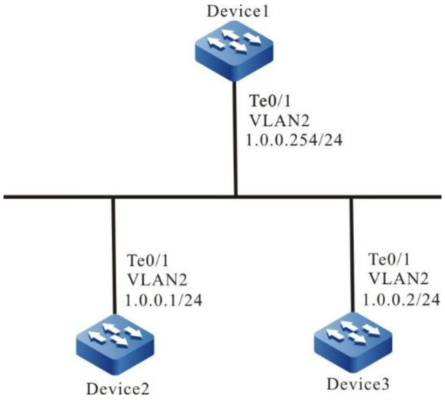


Figure 75-5 Configure NTP Broadcast Mode Networking

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Device1 sets the local clock as a reference with 3 layers. Configure Device1 as NTP broadcast server to send NTP broadcast packets on the interface VLAN2.

#Configure the local clock as a reference with 3 layers.

```
Device1#configure terminal
Device1(config)#ntp master 3
```

#Configure Device1 as NTP broadcast server to send NTP broadcast packets on the interface VLAN2.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ntp broadcast
```

Step 3: Configure Device2 as NTP broadcast client to monitor NTP broadcast packets on the interface VLAN2.

```
Device2#configure terminal
```

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ntp broadcast client
```

Step 4: Configure Device3 as NTP broadcast client to monitor NTP broadcast packets on the interface VLAN2.

```
Device3#configure terminal
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ntp broadcast client
```

Step 5: Check the result.

#On the client Device2, execute the **show ntp status** command to view the clock synchronization status and other information.

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D8E97C99.5110D9FE (03:27:21.316 Tue Apr 28 2015)
```

The number of clock layers of Device2 is 4, 1 more than that of Device1. The reference clock server address is 1.0.0.254, indicating that the client Device2 and the server Device1 have been synchronized.

#On the client Device2, execute the **show clock** command to view the Device clock.

```
Device2#show clock

BEIJING(UTC+08:00) TUE APR 28 11:27:22 2015
```

#On the client Device3, execute the **show ntp status** command to view the clock synchronization status and other information.

```
Device3#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D8E97CAC.78F42CA6 (03:27:40.472 Tue Apr 28 2015)
```

The number of clock layers of Device3 is 4, 1 more than that of Device1. The reference clock server address is 1.0.0.254, indicating that the client Device3 and the server Device1 have been synchronized.

#On the client Device3, execute the **show clock** command to view the Device clock.

```
Device3#show clock
```

```
BEIJING(UTC+08:00) TUE APR 28 11:27:41 2015
```

75.3.6 Configure NTP Broadcast Mode Authentication Function *-B -S -E -A*

Network Requirements

- Device1, Device2 and Device3 are interconnected through their respective interfaces, and the route is reachable.
- Device1 sets the local clock as a reference with 3 layers.
- Device1 is NTP broadcast server and enables NTP authentication to send NTP broadcast packets from the interface VLAN2.
- Device2 and Device3 are NTP broadcast clients, and enable NTP authentication to monitor NTP broadcast packets on their respective interface VLAN2.

Network Topology

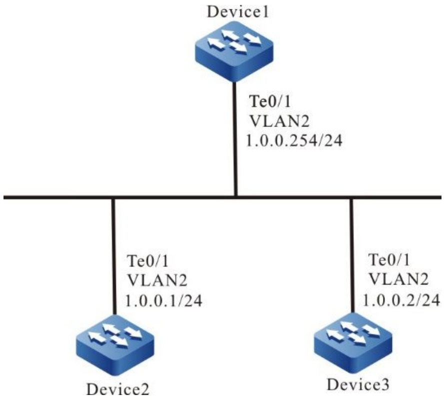


Figure 75-6 Configure NTP Broadcast Mode Authentication Function Networking

Configuration Steps

Step 1: Configure the interfaces' IP addresses. (omitted)

Step 2: Device1 sets the local clock as a reference with 3 layers. Configure Device1 as NTP broadcast server and configure MD5 authentication to send NTP broadcast packets on the interface VLAN2.

#Configure the local clock of the Device as a reference with 3 layers.

```
Device1#configure terminal
Device1(config)#ntp master 3
```

#Enable authentication.

```
Device1(config)#ntp authenticate
```

#The configuration authentication key sequence number is 1. The algorithm is MD5, and the key is admin.

```
Device1(config)#ntp authentication-key 1 md5 admin
```

#The key with configuration sequence number 1 is trusted.

```
Device1(config)#ntp trusted-key 1
```

NOTE

- The authentication sequence number of NTP client must be the same as that of the server with the same key.

#Enable the NTP broadcast server of the interface and specify that the key sequence number associated with the broadcast server is 1.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ntp broadcast key 1
```

Step 3: Configure Device2 as NTP broadcast client and configure MD5 authentication to monitor NTP broadcast packets on the interface VLAN2.

#Configure Device2 as Beijing time zone.

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING
```

#Enable authentication.

```
Device2(config)#ntp authenticate
```

#The configuration authentication key sequence number is 1. The algorithm is MD5, and the key is admin.

```
Device2(config)#ntp authentication-key 1 md5 admin
```

#The key with configuration sequence number 1 is trusted.

```
Device2(config)#ntp trusted-key 1
```

#Configure NTP broadcast client under the interface.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ntp broadcast client
```

NOTE

- To configure the NTP broadcast mode authentication function, it is necessary to specify the key sequence number associated with the server on the broadcast server, and there is no need to specify it on each broadcast client.

Step 4: Configure Device3 as NTP broadcast client and configure MD5 authentication to monitor NTP broadcast packets on the interface VLAN2.

#Configure Device3 as Beijing time zone.

```
Device3#configure terminal
```

```
Device3(config)#clock timezone BEIJING
```

#Enable authentication.

```
Device3(config)#ntp authenticate
```

#The configuration authentication key sequence number is 1. The algorithm is MD5, and the key is admin.

```
Device3(config)#ntp authentication-key 1 md5 admin
```

#The key with configuration sequence number 1 is trusted.

```
Device3(config)#ntp trusted-key 1
```

#Configure NTP broadcast client under the interface.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ntp broadcast client
```

NOTE

- To configure the NTP broadcast mode authentication function, it is necessary to specify the key sequence number associated with the server on the broadcast server, and there is no need to specify it on each broadcast client.

Step 5: Check the result.

#On the client Device2, execute the **show ntp status** command to view the clock synchronization status and other information.

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D90954DB.4DE52C7F (07:17:44.972 Fri May 22 2015)
```

The number of clock layers of Device2 is 4, 1 more than that of Device1, indicating that the broadcast client and NTP broadcast server Device1 have been synchronized.

#On Device2, execute the **show clock** command to view the Device clock.

```
Device2#show clock
BeiJing(UTC+08:00) FRI MAY 22 15:18:20 2015
```

#On the client Device3, execute the **show ntp status** command to view the clock synchronization status and other information.

```
Device3#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D90957A2.1B393E2D (07:22:10.106 Fri May 22 2015)
```

The number of clock layers of Device3 is 4, 1 more than that of Device1, indicating that the broadcast client and NTP broadcast server Device1 have been synchronized.

#On Device3, execute the **show clock** command to view the Device clock.

```
Device3#show clock
BeiJing(UTC+08:00) FRI MAY 22 15:22:15 2015
```

76 Port Mirror

76.1 Overview

76.1.1 Introduction to Port Mirror

Port mirror, also called SPAN (Switched Port Analyzer), is one management mode used to monitor the data flow of the device port. SPAN includes the local SPAN, remote SPAN and encapsulated remote SPAN.

76.1.2 Basic Concepts *-B -S -E -A*

SPAN Session

SPAN session means to mirror the data flow of one or multiple monitor ports on the device and send to the destination port. The mirrored data flow can be the input data flow and also can be the output data flow or mirror the input and output data flow at the same time. We can configure SPAN for the disabled port and the SPAN session does not take effect, but as long as the related port is enabled, SPAN takes effect.

Local SPAN

Local SPAN supports the port mirror on one device. All mirror ports and destination ports are on the same device.

Remote SPAN

Remote SPAN, also called RSPAN (Remote Switched Port Analyzer), supports that the mirror port can destination port are not on one device, realizing the remote monitoring across the L2 network. In the specified RSPAN VLAN, each RSPAN Session makes the mirror packets be forwarded in the L2 network. RSPAN includes RSPAN Source Session, RSPAN VLAN, and RSPAN Destination Session. We need to configure RSPAN source session and RSPAN destination session on different devices. When configuring the RSPAN source session, we need to specify one or multiple mirror ports and one RSPAN VLAN. The data mirrored by the monitor port is sent to RSPAN VLAN. To configure RSPAN destination session on another device, we need to specify the destination port and RSPAN VLAN. RSPAN destination session sends RSPAN VLAN data to the destination port.

Encapsulated Remote SPAN

Encapsulated remote SPAN, also called ERSPAN (Encapsulated Remote Switched Port Analyzer), encapsulates the mirror packets via the specified tunnel, traversing the L3 network, so as to mirror the data. ERSPAN includes ERSPAN Source Session and ERSPAN Destination Session. We need to configure ERSPAN Source Session and ERSPAN Destination Session on different devices. When configuring the ERSPAN source session, we need to specify one or multiple mirror ports, one source IP address, and destination IP address. Get the source MAC address according to the source IP address and get the next-hop MAC address according to the destination IP address; after the mirrored data is encapsulated with the information, send out from the next-hop egress port.

Traffic Type

Traffic type includes Receive (Rx) (the received traffic of the mirror port, Transmit (Tx) (the forwarded traffic of the mirror port, and Both (the received and forwarded traffic of the mirror port).

SPAN Source Port

SPAN source port is also called monitored port. Its data is monitored for network analysis. The monitored data flow can be at the input direction, output direction or both. It can function in different VLANs. The source port can be general port or aggregation group. One source port can only belong to one SPAN session.

SPAN Destination Port

SPAN destination port can only be one separate actual physical port or aggregation group. One destination port can only be used in one SPAN session. The destination port can be general port or aggregation group.

The device supports taking the destination port as the general forwarding port, but for universality and to make the monitored data not be interfered by other data flow, it is suggested to delete the destination port from all VLANs.

NOTE

- The destination port should not be connected to other device. Otherwise, it may result in the network loop.
- The destination port should be larger than or equal to the bandwidth of the mirror port. Otherwise, there may be packet loss.
- The destination port cannot enable LACP (Link Aggregation Control Protocol), so as to prevent the mirror data from being affected.

RSPAN VLAN

RSPAN VLAN should be one idle VLAN, specially used by RSPAN. We can select one idle VLAN during configuration, but should ensure that the other devices on the path from the mirror port to the destination port are all configured with the VLAN and add the corresponding ports of the other devices on the path to the VLAN.

76.2 SPAN Function Configuration

Table 76-1 SPAN Function Configuration List

Configuration Task	
Configure Local SPAN	Configure Local SPAN session
Configure RSPAN	Configure RSPAN VLAN
	Configure RSPAN source session
	Configure RSPAN destination session
Configure ERSPAN	Configure ERSPAN session

76.2.1 Configure Local SPAN *-B -S -E -A*

Local SPAN is used to analyze the data flow of the local device port.

Configuration Conditions

None

Configure Local SPAN Session

Local SPAN session copies the received or forwarded packets of one or multiple source ports and forwards out from the destination port without affecting the normal service forwarding of the source port.

Table 76-2 Configure the Local SPAN Session

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Configure the source end of Local SPAN session	**monitor session** *session-number* **source** { **interface** *interface-list* | **link-aggregation** *link-aggregation-id* } [**both** | **tx** | **rx**]	Mandatory By default, do not configure the source end of Local SPAN session.
Configure the destination end of the Local SPAN session	**monitor session** *session-number* **destination** { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* }	Mandatory By default, do not configure the destination end of the Local SPAN session.

NOTE

- When configuring the session source end and specifying the port enabled with the mirror as the aggregation group, the specified aggregation group should be already created. If the aggregation group is not created, the configuration fails. Similarly, when configuring the session destination end and specifying the forwarding port of the mirror packet as the aggregation group, the specified aggregation group also should be already created. If the aggregation group is not created, the configuration fails.
- One port cannot be the source port and destination port of one session at the same time.
- One port cannot exist in multiple sessions at the same time.

76.2.2 Configure RSPAN *-B -S -E -A*

RSPAN session is used to analyze the data flow of the source port of the reachable remote device at the L2 network. RSPAN session includes RSPAN source session and RSPAN destination session.

Configuration Conditions

None

Configure RSPAN VLAN

RSPAN makes the mirror packet traverse the L2 network by labeling the RSPAN LAN tag on the mirror packet.

Table 76-3 Configure RSPAN VLAN

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the VLAN configuration mode	**vlan** *vlan-id*	-
Configure the VLAN as RSPAN VLAN	**remote-span**	Mandatory By default, do not configure RSPAN VLAN.

NOTE

- RSPAN VLAN should not bear other services, but can only bear the RSPAN traffic.
- RSPAN VLAN prohibits enabling the MAC address learning function.
- Except for the ports used to bear the RSPAN traffic, do not configure any port to RSPAN VLAN.

Configure RSPAN Source Session

After configuring the RSPAN source session, label the RSPAN VLAN tag on the mirror packet and then forward it.

Table 76-4 Configure the RSPAN Source Session

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the source end of the RSPAN source session	**monitor session** *session-number* **source** { **interface** *interface-list* | **link-aggregation** *link-aggregation-id* } [**both | tx | rx**]	Mandatory By default, do not configure the source end of the RSPAN source session.
Configure the destination end of the RSPAN source session	**monitor session** *session-number* **destination remote vlan** *vlan* **interface** *interface-name*	Mandatory By default, do not configure the destination end of the RSPAN source session.

NOTE

- When configuring the session source end and specifying the port enabled with the mirror as the aggregation group, the specified aggregation group should be already created. If the aggregation group is not created, the configuration fails.
- The specified VLAN should be set as RSPAN VLAN before RSAPN source session.
- One port cannot be the source port and destination port of one session at the same time.
- One port cannot exist in multiple sessions at the same time.
- The destination end of RSPAN source session can only be the general port, but cannot be the aggregation group.

Configure RSPAN Destination Session

When RSPAN destination session receives the packet, identify the mirror packet according to the RSPAN VLAN tag, and forward the mirror packet to the analysis device.

Table 76-5 Configure the RSPAN Destination Session

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the source end of the RSPAN destination session	**monitor session** *session-number* **source remote vlan** *vlan-id*	Mandatory By default, do not configure the source end of the RSPAN destination session.
Configure the destination end of the RSPAN destination session	**monitor session** *session-number* **destination** { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* }	Mandatory By default, do not configure the destination end of the RSPAN destination session.

NOTE

- The session number in the source end configuration should be the same as the session number in the destination end configuration.
- The specified VLAN should be set as RSPAN VLAN before RSAPN destination session.
- One port cannot exist in multiple sessions at the same time.
- The type of the destination port of the RSPAN destination session should be Hybrid.

76.2.3 Configure ERSPAN *-A*

ERSPAN session is used to analyze the data flow passing the reachable remote device port of the L3 network.

Configuration Conditions

None

Configure ERSPAN Session

The destination end of the ERSPAN source session is used to specify the encapsulated source IP address, destination IP address, VLAN tag, TTL value, and TOS priority of the ERSPAN source session. After being encapsulated with the IP head, the mirror packet can traverse the L3 network.

Table 76-6 Configure the ERSPAN Source Session

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the source end of the ERSPAN source session	**monitor session** *session-number* **source** { **interface** *interface-list* | **link-aggregation** *link-aggregation-id* } [**both** | **tx** | **rx**]	Mandatory By default, do not configure the source end of the ERSPAN source session.
Configure the destination end of the ERSPAN source session	**monitor session** *session-number* **destination type erspan-source source-ip** *source-ip-addr* **destination-ip** *destination-ip-addr* [**vrf** *vrf-name*] [**vlan** *vlan-id*] [**ttl** *ttl*] [**tos** *tos*]	Mandatory By default, do not configure the destination end of the ERSPAN source session.

NOTE

- When configuring the session destination end and specifying the forwarding port of the mirror packet as the aggregation group, the specified aggregation group should be already created. If the aggregation group is not created, the configuration fails.
- The session number in the source end configuration should be the same as the session number in the destination end configuration.
- One port cannot exist in multiple sessions at the same time.
- Source IP address can directly search for the corresponding MAC address of the IP address.
- The specified source IP address is configured on the device.
- The next-hop egress port cannot belong to the aggregation group.

76.2.4 SPAN Monitoring and Maintaining *-B -S -E -A*

Table 76-7 SPAN Monitoring and Maintaining

Command	Description
show monitor rspan-vlan	Display RSPAN VLAN.

Command	Description
show monitor session { *session-number* | **all** | **local** | **remote | erspan** }	Display the SPAN session configuration information.

76.3 Typical Configuration Example of Port Mirror

76.3.1 Configure Local SPAN *-B -S -E -A*

Network Requirements

- PC1, PC2 and PC3 are connected with Device; PC1 and PC2 communicate with each other in VLAN2.
- Configure Local SPAN on Device; the source port is gigabitethernet0/1; the destination port is gigabitethernet0/3; PC3 monitors the packets received and sent by port gigabitethernet0/1 of Device.

Network Topology

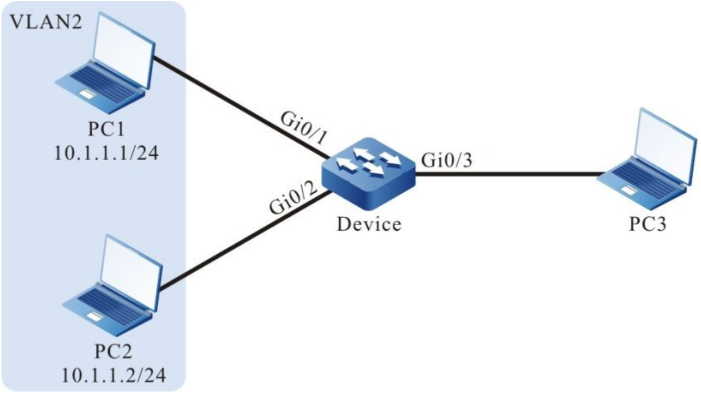


Figure 76-1 Networking of Configuring the Local SPAN

Configuration Steps

Step 1: Configure the link type of the VLAN and port.

#Create VLAN2 on Device.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure Local SPAN.

#Configure Local SPAN on Device, the mirror source session is port gigabitethernet0/1, and the destination session is port gigabitethernet0/3.

```
Device(config)#monitor session 1 source interface gigabitethernet 0/1 both
Device(config)#monitor session 1 destination interface gigabitethernet 0/3
```

#View the session information of Local SPAN on Device.

```
Device#show monitor session all
----------------------------------------------------------
Session 1
Type            : SPAN Local Session
Destination Interface : gigabitethernet0/3
Source Interface(both): gi0/1
```

Step 3: Check the result.

#When PC1 and PC2 communicate with each other, the packets sent and received by port gigabitethernet0/1 can be got on PC3.

76.3.2 Configure RSPAN *-B -S -E -A*

Network Requirements

- PC1 and PC2 are connected with Device1 and communicate with each other in VLAN2; PC3 is connected with Device2.
- Configure RSPAN on Device1 and Device2; PC3 monitors the packets received and sent by port gigabitethernet0/1 of Device1 via RSPAN VLAN3.

Network Topology

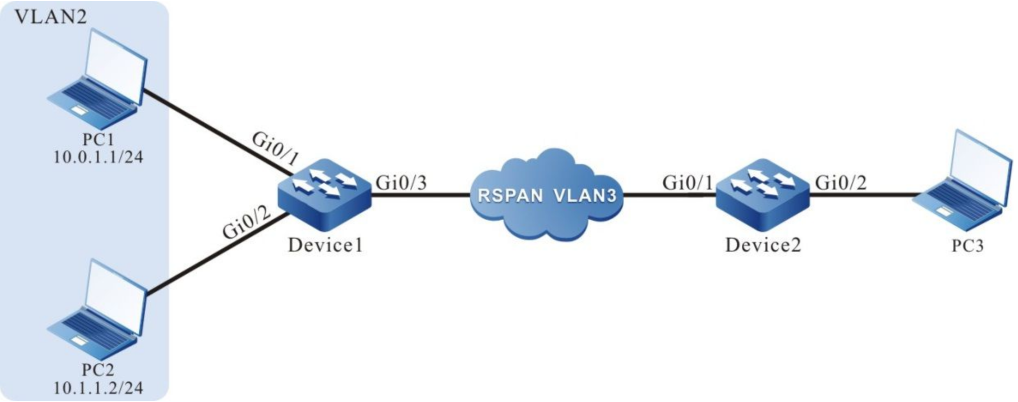


Figure 76-2 Networking of Configuring the RSPAN

Configuration Steps

Step 1: Configure the link type of the VLAN and port.

#Create VLAN2 on Device1.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device1 as Access, permitting the services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/1-0/2
Device1(config-if-range)#switchport mode access
Device1(config-if-range)#switchport access vlan 2
Device1(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/3 as Trunk on Device1.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode trunk
Device1(config-if-gigabitethernet0/3)#exit
```

#Configure the link type of port gigabitethernet0/1 as Trunk on Device2.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2 as Hybrid on Device2.

```
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode hybrid
Device2(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure RSPAN on Device1 and Device2.

#Configure VLAN3 as RSPAN VLAN on Device1 and configure port gigabitethernet0/3 to permit the services of VLAN3 to pass.

```
Device1(config)#vlan 3
Device1(config-vlan3)#remote-span
Device1(config-vlan3)#exit
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 3
Device1(config-if-gigabitethernet0/3)#exit
```

#Configure RSPAN on Device1, the mirror source session is port gigabitethernet0/1, and destination session is port gigabitethernet0/3.

```
Device1(config)#monitor session 1 source interface gigabitethernet 0/1 both
Device1(config)#monitor session 1 destination remote vlan 3 interface gigabitethernet 0/3
```

#View the RSPAN session information on Device1.

```
Device1#show monitor session all
-------------------------------------------------------
Session 1
Type            : RSPAN Source Session
RSPAN VLAN      : 3
Destination Interface : gigabitethernet0/3
Source Interface(both): gi0/1
```

#Configure VLAN3 as RSPAN VLAN on Device2 and configure port gigabitethernet0/1 to permit the services of VLAN3 to pass.

```
Device2(config)#vlan 3
Device2(config-vlan3)#remote-span
Device2(config-vlan3)#exit
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3
Device2(config-if-gigabitethernet0/1)#exit
```

#Configure RSPAN on Device2, the mirror source session is RSPAN VLAN3, and destination session is port gigabitethernet0/2.

```
Device2(config)#monitor session 1 source remote vlan 3
Device2(config)#monitor session 1 destination interface gigabitethernet 0/2
```

#View the RSPAN session information on Device2.

```
Device2#show monitor session all
--------------------------------------------------------
Session 1
Type            : RSPAN Destination Session
RSPAN VLAN      : 3
Destination Interface : gigabitethernet0/2
```

Step 3: Check the result.

#When PC1 and PC2 communicate with each other, the packets sent and received by port gigabitethernet0/1 of Device1 can be got on PC3.

76.3.3 Configure ERSPAN *-A*

Network Requirements

- PC1 and PC2 are connected with Device1 and communicate with each other in VLAN2.
- PC3 communicates with Device via IP Network.
- Configure ERSPAN on Device; the source IP address is 192.168.1.1/24; the destination IP address is 192.168.2.2/24; PC3 monitors the packets received and sent by port gigabitethernet0/1 of Device.

Network Topology

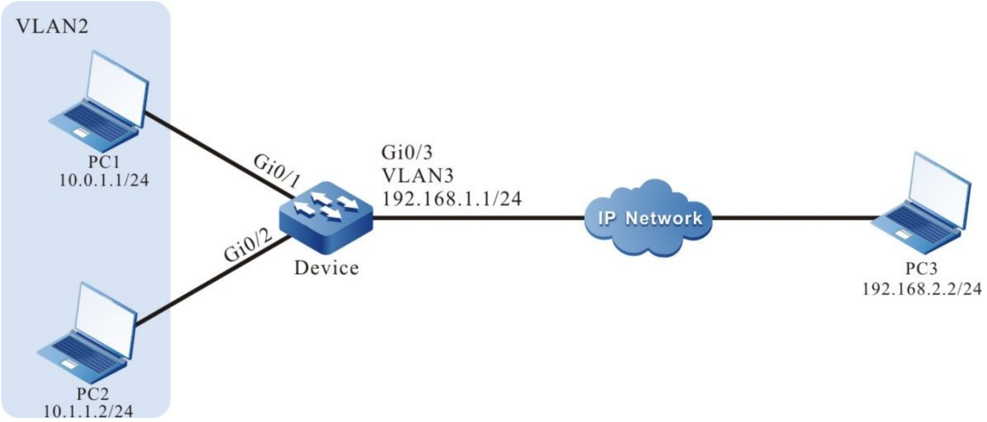


Figure 76-3 Networking of Configuring the ERSPAN

Configuration Steps

Step 1: Configure VLAN, port link type and interface address.

#Create VLAN2 and VLAN3 on Device.

```
Device#configure terminal
Device(config)#vlan 2-3
```

#Configure the link type of port gigabitethernet0/1 and gigabitethernet0/2 on Device as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/3 on Device as Access, permitting the services of VLAN3 to pass.

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

#Configure the interface IP address on Device.

```
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 192.168.1.1 255.255.255.0
Device(config-if-vlan3)#exit
```

Step 2: Configure the route to segment 192.168.2.0/24 on Device. (Omitted)

Step 3: Configure ERSPAN on Device.

#Configure ERSPAN on Device, the mirror source session port is gigabitethernet0/1, the source IP address of the destination session is 192.168.1.1, and the destination IP address is 192.168.2.2.

```
Device(config)#monitor session 1 source interface gigabitethernet 0/1 both
Device(config)#monitor session 1 destination type erspan-source source-ip 192.168.1.1 destination-ip
192.168.2.2 vlan 3
```

#View the ERSPAN session information on Device.

```
Device#show monitor session all
-----------------------------------------------------------
Session 1
Type            : ERSPAN Source Session
Destination Interface : gigabitethernet0/3
Source Interface(both): gi0/1
Source IP Address: 192.168.1.1
Destination IP Address: 192.168.2.2
Source Mac Address: 94ae.e354.5c94
Next Hop Mac Address: 0000.1100.0001
Erspan L2 Vlan:3
```

Step 4: Check the result.

#When PC1 and PC2 communicate with each other, the packets sent and received by port gigabitethernet0/1 can be got on PC3.

77 sFlow

77.1 Overview

sFlow is one technology used to sample and monitor the network traffic, complying with the RFC3176 standard. sFlow performs different samplings according to different configurations. The sampling process is: First analyze the packet head from the sampled packet, encapsulate as the sFlow packet according to the standard definition, and send to the third-party receiver, which is convenient for the user to analyze and monitor the traffic entering the device via the third-party receiver.

sFlow includes the following two sampling modes:

- Sampler sampling mode: It is one sampling mode provided by the switching chip, sampling the traffic entering the port at random;
- Poller sampling mode: It is one software sampling mode, used to collect the packet and traffic statistics information of the port regularly.

sFlow defines the following two roles:

- Agent role: It is the sFlow agent on the device, used to manage the two sampling modes of sFlow and execute the sampling task;
- Receiver role: It is the mapping of the third-party receiver supporting the sFlow protocol on the local device, used to save the information of the third-party receiver (such as IP address and UDP port number) and regularly send the sFlow packets buffered on the device to the third-party receiver.

77.2 sFlow Function Configuration

Table 77-1 sFlow Function Configuration List

Configuration Task	
Configure the sFlow basic functions	Create the agent role
	Create the receiver role
Configure sFlow sampling mode	Configure the sampler sampling mode
	Configure the poller sampling mode

77.2.1 Configure sFlow Basic Functions *-B -S -E -A*

Configuration Conditions

Before configuring the sFlow basic functions, first complete the following task:

- Create the VLAN interface on the device and configure the IP address, making the device and the third-party receiver reachable

Create agent Role

The agent role is used to configure and manage the sampling. Currently, only IPv4 address is available for the agent role.

Table 77-2 Create the Agent Role

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the agent role	**sflow agent ip** *ip-address*	Mandatory By default, do not create the agent role.

Create receiver Role

The receiver role is used to save the information of the third-party receiver and send the sFlow packets buffered on the device to the third-party receiver via the UDP mode. The triggering conditions of sending packets include the following two:

- When the specified buffer area is full and cannot be filled with new sFlow sampling information, first encapsulate the buffered part to the sFlow packet, send to the third-party receiver, and then fill the new part to the buffer area. This can reduce the number of the sFlow packets sent by the device to the third-party receiver obviously.
- Encapsulate the buffered sFlow sampling information as the sFlow packet periodically and send to the third-party receiver. This can avoid that the buffered part cannot be encapsulated as the sFlow packet and sent to the third-party receiver because of not receiving new sFlow sampling information within a long time.

Table 77-3 Create the Receiver Role

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the receiver role	**sflow receiver** *receiver-index* **owner** *owner-name* **ip** *ip-address* [**packet-size** *packet-size-value* **timeout** *timeout-value*	Mandatory By default, do not create the receiver role.

Step	Command	Description
	udp-port *udp-port-number*]	

77.2.2 Configure sFlow Sampling Mode *-B -S -E -A*

Configuration Conditions

Before configuring the sFlow sampling mode, first complete the following task:

- Create the agent role
- Create the receiver role

Configure sampler Sampling Mode

In the sampler sampling mode, that is port flow sampling, the switching chip samples the traffic received by the port at random. After getting the sample packet, first copy the head information of the packet, resolve the copied content, get the desired sample information from it, and at last, encapsulate the sample information and send to the corresponding third-party receiver of the receiver role.

Table 77-4 Configure the Port Sampler Sampling Mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the sampler sampling mode	**sflow sampler receiver** *receiver-index* [**header-size** *header-size-value* **sample-rate** *sample-rate-value* **direction** *direction-value* **type** *type-value*]	Mandatory By default, do not configure the sampler sampling mode.

Configure poller Sampling Mode

The poller sampling mode, that is port regular polling sampling, is to regularly encapsulate the packet and traffic statistics information on the port within the period and send to the corresponding third-party receiver of the receiver role.

Table 77-5 Configure the poller Sampling Mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	-
Configure the poller sampling mode	**sflow poller** *poller-index* **receiver** *receiver-index* [**interval** *interval-value* **type** *type-value*]	Mandatory By default, do not configure the poller sampling mode.

77.2.3 sFlow Monitoring and Maintaining ***-B -S -E -A***

Table 77-6 sFlow Monitoring And Maintaining

Command	Description
clear sflow receiver *receiver-index* **statistics**	Clear the sFlow sampling statistics information related with the specified receiver role
show sflow	Display the sFlow configuration and running information
show sflow agent	Display the configuration and running information of the agent role
show sflow poller [**interface** *interface-name*]	Display the configuration and running information of the poller sampling mode on the port
show sflow receiver [*receiver-index* [**statistics**]]	Display the sFlow sampling statistics information, configuration and running information related with the receiver role
show sflow sampler [**interface** *interface-name*]	Display the configuration and running information of the sampler mode on the port

77.3 sFlow Typical Configuration Example

77.3.1 Configure sFlow Basic Functions *-B -S -E -A*

Network Requirements

- Device is the sFlow agent device and the route with the NMS server is reachable.
- The NMS server monitors the port data traffic of Device via sFlow.

Network Topology

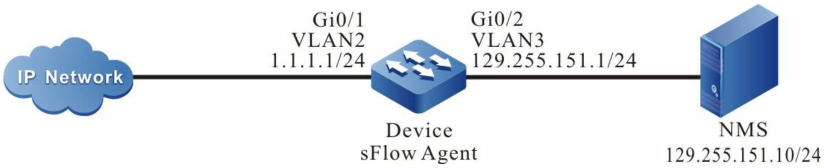


Figure 77-1 Networking of Configuring the sFlow Basic Functions

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the sFlow function.

#Enable the sFlow agent.

```
Device#configure terminal
Device(config)#sflow agent ip 1.1.1.1
```

#Configure the destination IP address and destination UDP port number of the sFlow statistics output packet, the interval of sending packet is 5s, and the buffer size is 1400 bytes.

```
Device(config)#sflow receiver 1 owner 1 ip 129.255.151.10 timeout 5 udp-port 6343 packet-size 1400
```

#Perform the sampler sampling for the ingress flow of port gigabitethernet0/1 and the sampling frequency is 10.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#sflow sampler receiver 1 sample-rate 10 direction rx
```

#Perform the poller sampling for the ingress flow of port gigabitethernet0/1 and the polling period is 20s.

```
Device(config-if-gigabitethernet0/1)#sflow poller 1 receiver 1 interval 20
Device(config-if-gigabitethernet0/1)#exit
```

Step 4: Check the result.

#View the sFlow information on Device.

```
Device#show sflow

sFlow Agent Configuration: (Interval = 120, Current Tick = 0x002a6476)
```

```
              Address                          Receivers   Samplers    Pollers
 Version   Id  Type       Net Address     Socket   Number      Number      Number      Boot Time / Exec Time
--------- ---- ------- ----------------- -------- ----------- ----------- ----------- -----------/-----------
 1.3        1   IPv4    1.1.1.1          0x1c     1/78        1/156       1/156       0x00000ab2/0x002a644c


sFlow Receivers Configuration: (Reset Delta = 18000, Current Tick = 0x002a6476)

                                                          Datagram Maximum
 Index           Owner              Net Address      Port   Version  Datagram Timeout Reset Time /Expire Time
------- ------------------------- ----------------- ------- -------- -------- ------- -----------/-----------
     1   1                       129.255.151.10     6343       5     1400       5   0x002a644c/0x002a6578



sFlow Samplers Configuration:


 Sampling Types: H - raw packet header  E - ethernet packet
                 F - IPv4 packet        S - IPv6 packet


              Receiver Sampling Sampling  Maximum Sampling   Pkts Number
  Interface   Index    Rate     Direction Header  Types      (Curr/Last)
------------- -------- -------- --------- ------- -------- ---------------
 gi0/1            1       10   rx         128   H       0x0000/0x0001



sFlow Pollers Configuration: (Current Tick = 0x002a6476)


 Sampling Types: G - generic counter
                 E - ethernet counter


                      Receiver Sampling
  Interface   Instance Index    Types     Interval  Countdown
------------- -------- -------- -------- -------- ------------
 gi0/1            1        1   G           10   0x002a65b4
```

#On NMS, we can view the ingress flow information of port gigabitethernet0/1 on Device.

78 LLDP

78.1 Overview

78.1.1 Overview of LLDP Protocol *-B -S -E -A*

LLDP (Link Layer Discovery Protocol) is the link layer protocol defined in the IEEE 802.1ab standard. It organizes the information of the local device to TLV (Type/Length/Value), encapsulates in LLDPDU (Link Layer Discovery Protocol Data Unit) and sends to the direct-connected neighbor device. Meanwhile, it saves the LLDPDU received from the neighbor device in the standard MIB (Management Information Base) mode. With LLDP, the device can save and manage its own and direct-connected neighbor device information for the network management system to query and judge the link communication status.

78.1.2 TLV Type Information *-B -S -E -A*

TLV that LLDP can encapsulate includes the basic TLV, organization-defined TLV and MED (Media Endpoint Discovery) TLV. Basic TLV is a group of TLV regarded as the basis of the network device management. Organization defined TLV and MED TLV is the TLV defined by the standard organization and other institutions, used to strengthen the management for the network devices. We can configure whether to release in LLDPDU according to the actual demand.

Basic TLV

In basic TLV, there are several types of TLV, which are mandatory for realizing the LLDP function, that is, should release in LLDPDU, as shown in the following table.

Table 78-1 Description of the Basic TLV

TLV Type	Description	Whether to release
End of LLDPDU TLV	Indicate LLDPDU end	Yes
Chassis ID TLV	The MAC address of the sending device	Yes
Port ID TLV	Used to identify the port of the LLDPDU sending end; when the device does not send MED TLV, the content is the port name; when selecting to send MED TLV, the content is	Yes

TLV Type	Description	Whether to release
	the MAC address of the port.	
Time To Live TLV	The live time of the local device information on the neighbor device	Yes
Port Description TLV	The description character string	No
System Name TLV	The device name	No
System Description TLV	The system description	No
System Capabilities TLV	The main functions of the system and which functions can be enabled	No
Management Address TLV	Management address, and the corresponding interface number and OID (Object Identifier); the management address is permitted by the interface to pass and is the main IP address of the VLAN with the minimum VLAN ID; if the VLAN with the minimum VLAN ID is not configured with the main IP address, the management address value is 127.0.0.1.. By default, send the TLV.	Yes

Organization-defined TLV

The organization-defined TLV includes the 802.1 organization-defined TLV and 802.3 organization-defined TLV, as shown in the following table.

Table 78-2 The Description of 802.1 Organization-defined TLV

TLV Type	Description	Whether to release
Port VLAN ID TLV	Port VLAN ID	No

TLV Type	Description	Whether to release
Port And Protocol VLAN ID TLV	The protocol VLAN ID of the port	No
VLAN Name TLV	The port VLAN name	No
Protocol Identity TLV	The protocol type supported by the port. The local device does not support sending Protocol Identity TLV, but can receive the type of TLV.	No

Table 78-3 The Description of the 802.3 Organization-defined TLV

TLV Type	Description	Whether to release
MAC/PHY Configuration/Status TLV	The rate and duplex status of the port, whether to support the auto negotiation of the port rate, whether to enable the auto negotiation function, and the current rate and duplex status	No
Power Via MDI TLV	The power supply capability of the port	No
Link Aggregation TLV	Whether the port supports the link aggregation and whether to enable the link aggregation	No
Maximum Frame Size TLV	The supported maximum frame length, using the configured MTU of the port (Max Transmission Unit)	No

MED TLV

The MED TLV information is as shown in the following table.

Table 78-4 The Description of MED TLV

TLV Type	Description	Whether to release
LLDP-MED Capabilities TLV	The MED device type of the device and the LLDP MED TLV type that can be encapsulated in LLDPDU	No
Network Policy TLV	The port VLAN ID, supported application (such as voice and video), application priority and used policy information	No
Extended Power-via-MDI TLV	The power supply capability of the device	No
Hardware Revision TLV	The hardware version of the device	No
Firmware Revision TLV	The firmware version of the device	No
Software Revision TLV	The software version of the device	No
Serial Number TLV	The serial number of the device	No
Manufacturer Name TLV	The manufacturer of the device	No
Model Name TLV	The module name of the device	No
Asset ID TLV	The asset ID of the device for directory management and asset tracking	No
Location Identification TLV	The location ID information of the connected device, used by the other devices in the application based on the location	No

78.1.3 LLDP Work Mechanism *-B -S -E -A*

LLDP Work Mode

The port includes the following four LLDP work modes:

- RxTx: send and receive LLDPDU;
- Tx: only send LLDPDU;
- Rx: only receive LLDPDU;
- Disable: do not send or receive LLDPDU.

LLDP Sending Mechanism

The LLDP sending mechanism:

- When the port works in the RxTx or Tx mode, regularly send LLDPDU to the neighbor device according to the sending period of the LLDP packet;
- After the port enables the polling function, regularly poll whether the LLDP concerned configuration in the local device changes. If the configuration changes, send LLDPDU at once. To prevent the frequent change of the local information from causing lots of the sent LLDPDU, it is necessary to delay and wait for some time and then continue to send the next LLDPDU when sending one LLDPDU every time.
- When some configuration related with the local device LLDP changes (for example, select the released TLV type), or if finding the configuration change after enabling the polling function, enable the fast sending mechanism, that is, immediately send the LLDPDU of the specified quantity continuously, and then restore the normal LLDP packet sending period.
- When the global LLDP function is disabled or the port enabled with LLDP executes shutdown, adds to the aggregation group, and disables the LLDP, as well as restarts the device, send one LLDPDU with CLOSE TLV to inform the neighbor device.

LLDP Receiving Mechanism

When the port works in the RxTx or Rx mode, check the validity of the received LLDPDU and the carried TLV. After passing the validity check, save the neighbor information to the local device and set the age time of the neighbor information at the local device according to the TTL (Time To Live) carried in LLDPU. If the TTL value in the received LLDPDU is 0, age the neighbor information at once. The storing capability of the LLDP protocol for the neighbor is limited. Currently, one port of the device supports the information of 20 neighbors at most. The device can store 2000 neighbors at most. If the neighbors reach the threshold, more neighbor advertising packets are dropped and cannot be saved.

78.2 LLDP Function Configuration

Table 78-5 LLDP Function Configuration List

Configuration Task	
Configure the LLDP basic functions	Enable the global LLDP function

Configuration Task	
	Enable the port LLDP function
Configure the LLDP work mode	Configure the LLDP work mode
Configure the TLV that LLDP permits to release	Configure the basic TLV permitted to release
	Configure the organization-defined TLV permitted to release
	Configure the MED TLV permitted to release
Configure the LLDP parameters	Configure the neighbor live time
	Configure the period of sending packets
	Configure the number of the packets sent fast
	Configure the re-initializing delay
	Configure the period of checking the LLDP configuration

78.2.1 Configure LLDP Basic Functions *-B -S -E -A*

Enable the global LLDP function and port LLDP function at the same time so that LLDP can work normally. The local device gets the neighbor device information by interacting LLDPDU with other device.

Configuration Conditions

None

Enable Global LLDP Function

Table 78-6 Enable the Global LLDP Function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the global LLDP function	**lldp run**	Mandatory

Step	Command	Description
		By default, do not enable the global LLDP function.

Enable Port LLDP Function

Table 78-7 Enable the Port LLDP Function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enable the port LLDP function	**lldp enable**	Mandatory By default, do not enable the port LLDP function.

78.2.2 Configure LLDP Work Mode *-B -S -E -A*

Configuration Conditions

None

Configure LLDP Work Mode

The user can set different work modes according to the role of the device in the network. If it is the seed device (the center device collected by network topology), it is suggested to configure the LLDP work mode as Rx. Otherwise, it is suggested to configure the LLDP work mode as Tx.

Table 78-8 Configure the LLDP Work Mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the LLDP work mode as Rx	**lldp receive**	Optional By default, LLDP work mode is RxTx. LLDP work mode is decided by the command **lldp receive** and **lldp transmit** together.
Configure the LLDP work mode as Tx	**lldp transmit**	

78.2.3 Configure TLV LLDP Permits to Release *-B -S -E -A*

The neighbor device can get to know the details of the local device by releasing TLV.

Configuration Conditions

None

Configure Basic TLV LLDP Permits to Release

The user can release different basic TLVs according to the actual application demand.

Table 78-9 Configure the Basic TLV LLDP Permits to Release

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface

Step	Command	Description
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Configure the basic TLV LLDP permits to release	**lldp tlv-select** { **basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **| dot1-tlv** { **all | port-vlan-id | protocol-vlan-id | vlan-name** } **| dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power** } }	Optional By default, permit to release all basic TLVs.

Configure Organization-defined TLV LLDP Permits to Release

The user can release different organization-defined TLVs according to the actual application demand.

Table 78-10 Configure the Organization-Defined TLV LLDP Permits to Release

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface i***nterface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the organization-defined TLV LLDP permits to release	**lldp tlv-select** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** | **vlan-name** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } }	Optional By default, permit to release all organization-defined TLVs.

Configure MED TLV LLDP Permits to Release

The user can release different MED TLVs according to the actual application demand.

Table 78-11 Configure the MED TLV LLDP Permits to Release

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Configure the MED TLV LLDP permits to release	**lldp med-tlv-select** { **all** | **capability** | **location-id elin-address** *phonenum* | **network-policy** | **power-via-mdi** | **inventory** }	Optional By default, do not permit to release all MED TLVs.

78.2.4 Configure LLDP Parameters *-B -S -E -A*

Configuration Conditions

None

Configure Neighbor Life Time

Specify the life time of the local device information on the neighbor device by configuring the neighbor TTL so that the neighbor device can delete the local device information after the TTL of the local device arrives.

Table 78-12 Configure the Neighbor Life Time

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the life time of the local device on the neighbor device	**lldp holdtime** *holdtime-value*	Optional By default, the life time of the local device on the neighbor device is 120s.

Configure Packet Sending Period

The local device regularly sends the LLDP packet to the neighbor device by configuring the period of sending the packets so that the information of the local device on the neighbor device is not aged.

Table 78-13 Configure the Period of Sending Packets

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the period of sending the LLDP packets	**lldp transmit-interval** *transmit-interval-value*	Optional By default, the period of sending the LLDP packets is 30s.

Configure Fast Sent Packet Quantity

When some LLDP configuration of the local device (for example, select the released TLV type) changes, or when the polling mechanism finds that the LLDP concerned configuration information in the local device changes after enabling the polling function, to make other devices discover the change of the local device as soon as possible, enable the fast sending mechanism, that is, continuously send the

LLDPDUs of the specified quantity (it is 3 by default) at once, and then restore the normal sending period.

Table 78-14 Configure the Fast Sent Packet Quantity

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the number of the fast sent packets	**lldp fast-count** *fast-count-value*	Optional By default, the number of the fast sent packets is 3.

Configure Re-initializing Delay

When the port work mode changes, re-initialize the port protocol status machine. To prevent the frequent change of the port work mode from re-initializing the port protocol status machine continuously, we can configure the re-initializing delay of the port.

Table 78-15 Configure the Re-initializing Delay

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the re-initializing delay	**lldp reinit** *reinit-value*	Optional By default, the re-initializing delay is 2s.

Configure LLDP Configuration Check Period

To inform the neighbor device in time after the LLDP configuration changes, we can configure the period of checking the LLDP configuration.

Table 78-16 Configure the Period of Checking the LLDP Configuration

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the L2 Ethernet interface configuration mode	**interface** *interface-name*	Either After entering the L2 Ethernet interface

Step	Command	Description
Enter the aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	configuration mode, the subsequent configuration takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enable the polling function and configure the polling period	**lldp check-change-interval** *check-change-interval-value*	Optional By default, the polling function is disabled.

78.2.5 LLDP Monitoring and Maintaining *-B -S -E -A*

Table 78-17 LLDP Monitoring and Maintaining

Command	Description
clear lldp neighbors	Clear the neighbor information of all ports
show lldp neighbors [**detail** | **interface** *interface-name* [**detail**] | **link-aggregation** *link-aggregation-id* [**detail**]]	Display the neighbor information
clear lldp statistics	Clear the LLDP packet statistics information
show lldp statistics { **interface** *interface-name* | **link-aggregation** *link-aggregation-id* }	Display the received and sent LLDP packet statistics information of the specified port
show lldp	Display the LLDP global configuration information
show lldp interface *interface-name*	Display the LLDP work mode of the specified port and the polling period of checking the LLDP configuration change
show lldp link-aggregation *link-aggregation-id*	Display the LLDP work mode of the specified aggregation group and the polling period of checking the LLDP configuration change

Command	Description
show lldp tlv-select [**interface** *interface-name* | **link-aggregation** *link-aggregation-id*]	Display the basic TLV and organization-defined TLV configuration information

78.3 LLDP Typical Configuration Example

78.3.1 Configure LLDP Basic Functions *-B -S -E -A*

Network Requirements

- Configure the LLDP function on Device1, Device2 and Device3, realizing the link-layer neighbor discovery.

Network Topology

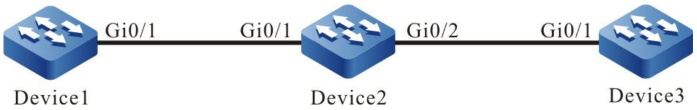


Figure 78-1 Networking of Configuring the LLDP Basic Functions

Configuration Steps

Step 1: Enable the LLDP function on Device.

# Enable the LLDP function on Device1.

```
Device1#configure terminal
Device1(config)#lldp run
```

#Enable the LLDP function on Device2.

```
Device2#configure terminal
Device2(config)#lldp run
```

#Enable the LLDP function on Device3.

```
Device3#configure terminal
Device3(config)#lldp run
```

Step 2: Configure the LLDP function on the port.

#Enable the LLDP function on port gigabitethernet0/ of Device1.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#lldp enable
Device1(config-if-gigabitethernet0/1)#exit
```

#Enable the LLDP function on port gigabitethernet0/ of Device2.

```
Device2(config)#interface gigabitethernet 0/1
```

```
Device2(config-if-gigabitethernet0/1)#lldp enable
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#lldp enable
Device2(config-if-gigabitethernet0/2)#exit
```

#Enable the LLDP function on port gigabitethernet0/ of Device3.

```
Device3(config)#interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#lldp enable
Device3(config-if-gigabitethernet0/1)#exit
```

Step 3:   Check the result.

#View the neighbor information on Device1.

```
Device1#show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID        Local Intf      Hold-time  Capability    Peer Intf
Device2          gi0/1           120        P,R,          gi0/1
```

Device2 discovers neighbor Device2.

#View the details of Device1 neighbor.

```
Device1#show lldp neighbors detail

Chassis ID: 94ae.e354.5ca5
Interface ID: gi0/1
Interface Description: gigabitethernet0/1
System Name: Device2

System Description: Hirschmann IT (R) Operating System Software

Time remaining: 100 seconds
System Capabilities: P,R,
Enabled Capabilities: P,R,
Management Addresses:
    IP : 127.0.0.1
Auto Negotiation - supported, enabled
Max Translate Unit: 1824
Media Attachment Unit type: 30
---------------------------------------------


Total entries displayed: 1
```

NOTE

- For viewing the neighbor information of Device2 and Device3, refer to Device1.

79 SNMP

79.1 Overview

SNMP (Simple Network Management Protocol) is one standard protocol of managing Internet. It ensures that the management information can be transmitted between Network Managing Station and managed device SNMP agent. It is convenient for the system administrator to manage the network system.

SNMP is one application layer protocol in the client/server mode. It mainly includes three parts:

- NMS (Network Managing Station)
- SNMP agent
- MIB (Management Information Base).

The structure set of all managed objects maintained by the device is called MIB. The managed objects are organized according to the hierarchical tree structure. MIB defines the network management information got by one device. To be consistent with the standard network management protocol, each device should use the format defined in MIB to display the information. One subset of IOS ASN.1 defines the syntax for MIB. Each MIB uses the tree structure defined in ASN.1 to organize all available information. Each piece of information is one node with punctuation and each node contains one object ID and one short text description.

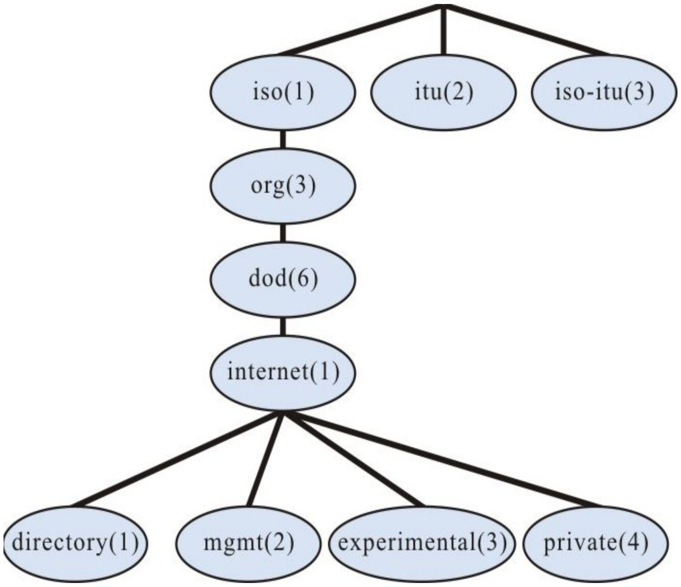


Figure 79–1 ASN.1 Tree Diagram of Network Management

SNMP protocol versions include SNMPv1, SNMPv2, and SNMPv3.

- SNMPv1: The first version of the SNMP protocol. The disadvantages: security problem, bandwidth waste, no communication capability between managers, the protocol only provides the limited operations;

- SNMPv2: It makes some improvement on the basis of SNMPv1, making the functions stronger and the security better;
- SNMPv3: original identity, information integrality and some aspects of re-transmission protect, content confidentiality, authorization and process control, the remote configuration and management capability needed by the above three capabilities;

Therefore, the development of SNMPv3 is centralized on two targets, that is, provide the workable security platform at the enhanced architecture and maintain the consistency of the network management system.

The SNMP protocol mainly includes the following operations:

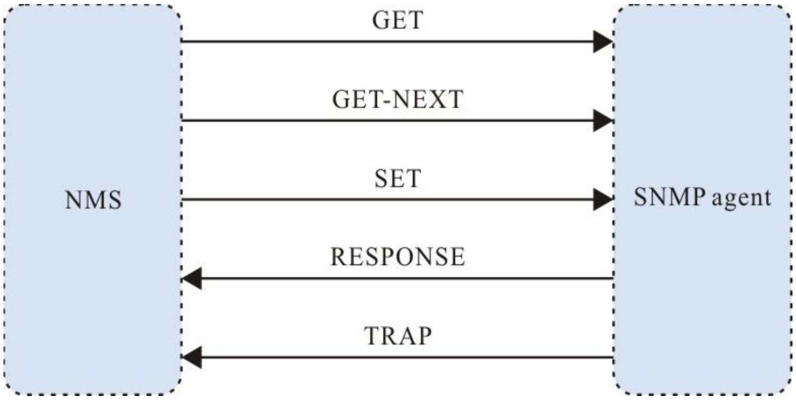


Figure 79–2 SNMP Management Operation Diagram

- Get-request: SNMP network work station gets one or multiple parameters from the SNMP agent.
- Get-next-request: SNMP network work station gets the next parameter of one or multiple parameters from the SNMP agent.
- Get-bulk: SNMP network work station gets the batch parameters from the SNMP agent.
- Set-request: SNMP network work station sets one or multiple parameters of the SNMP agent.
- Get-response: SNMP agent returns one or multiple parameters and it is the responding operation of the SNMP agent for the above three operations.
- Trap: The packet sent by the SNMP agent actively, informing that something happens to the SNMP network work station.

SNMPv1 and SNMPv2 use the authentication name to check whether to have the right to use the MIB object, so only when the authentication name of the network work station is consistent with one authentication name defined in the device, we can manage the device.

The authentication name has the following two attributes:

- Read-only: The read authority of the authorized network work station for all MIB objects of the device;
- Read-write: The read and write authority of the authorized network work station for all MIB objects of the device.

SNMPv3 determines which security mechanism to be adopted to process the data by the security model and the security level. There are three security models: SNMPv1, SNMPv2c, and SNMPv3.

Table 79–1 Supported Security Model and Security Level

Security Model	Security Level	Authentication	Encryption	Description
SNMPv1	NoAuthNoPriv	Authentication name	None	Confirm the data validity via the authentication name.
SNMPv2c	NoAuthNoPriv	Authentication name	None	Confirm the data validity via the authentication name.
SNMPv3	NoAuthNoPriv	User name	None	Confirm the data validity via the user name.
SNMPv3	AuthNoPriv	MD5/SHA	None	Use HMAC-MD5/HMAC-SHA data authentication mode.
SNMPv3	AuthPriv	MD5/SHA	DES	Use the HMAC-MD5/HMAC-SHA data authentication mode and CBC-DES data encryption mode.

79.2 SNMP Function Configuration

Table 79–2 SNMP Function Configuration List

Configuration Task	
Configure the SNMP basic functions	Enable the SNMP service
	Configure the MIB view
	Configure the manager contact information
	Configure the physical location information of the device
Configure SNMPv1/v2	Configure the SNMP community name
	Configure the SNMP Trap functions
Configure SNMPv3	Configure the SNMP user group

Configuration Task	
	Configure the SNMP user
	Configure SNMP advertising
	Configure SNMP agent forwarding

79.2.1 Configure SNMP Basic Functions *-B -S -E -A*

Configuration Conditions

None

Enable SNMP Service

If the device is enabled with the SNMP service, the device can manage and configure via the SNMP network management software.

Table 79–3 Enable the SNMP Service

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Enable the SNMP service	**snmp-server start [rfc]**	Mandatory By default, the SNMP service is disabled.

Configure MIB View

Use the view-based access control model to judge whether the associated management object of one operation is permitted by the view. Only the management objects permitted by the view can be permitted to access.

Table 79–4 Configure the MIB View

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Configure the MIB view	**snmp-server view** *view-name oid-string* { **include** | **exclude** }	Mandatory By default, the SNMP view name is Default.

Configure Manager Contact Information

The manager contact information is one information node in the SNMP protocol. The network management software can get the information via SNMP.

Table 79–5 Configure the Manager Contact Mode

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Configure the manager contact information	**snmp-server contact** *contact-line*	Mandatory

Configure Device Physical Location Information

The device physical location information is one information node in the SNMP protocol. The network management software can get the information via SNMP.

Table 79–6 Configure the Physical Location Information of the Device

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Configure the physical location information of the device	**snmp-server location** *location*	Mandatory

79.2.2 Configure SNMPv1/v2 ***-B -S -E -A***

Configuration Conditions

Before configuring SNMPv1/v2, first complete the following task:

- Configure the link-layer protocol, ensuring the normal communication of the link layer
- Configure the IP address of the interface, making the network layer of the neighboring nodes reachable

Create SNMP Community Name

SNMPv1/SNMPv2c adopts the security scheme based on the community name. SNMP community name can be regarded as the password between NMS and SNMP proxy, that is to say, SNMP proxy only accepts the management operations of the same community name and the SNMP from different community name is not responded and is dropped directly.

Table 79–7 Configure the Community Name

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Configure the community name of the SNMP proxy	**snmp-server community** *community-name* [**view** *view-name*] { **ro** | **rw** } [*access-list-number*]	Mandatory By default, the community name is public.

79.2.3 Configure SNMPv3 *-B -S -E -A*

Configuration Conditions

Before configuring SNMPv3, first complete the following task:

- Configure the link-layer protocol, ensuring the normal communication of the link layer
- Configure the IP address of the interface, making the network layer of the neighboring nodes reachable

Create SNMP User Group

During controlling, we can associate some user with one group. The users of one group have the same access authority.

- We can configure one group to associate with the view. There are three kinds of views, that is, read-only view, write view and notify view.
- We can configure the security level of the group, configuring whether to need the authentication and encryption.

Table 79–8 Create the SNMP User Group

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Create the SNMP user group	**snmp-server group** *group-name* **v3** { **authnopriv** | **authpriv** | **noauth** } [**notify** *notify-view* | **read** *read-view* | **write** *write-view*]	Mandatory **Authnopriv:** authenticate, but not encrypt **Authpriv:** authenticate and encrypt **Noauth:** not authenticate or encrypt

Create SNMP User

Perform the security management via the user-based security model. The network work station can communicate with the SNMP proxy only after using the valid user. The valid user needs to be configured.

For SNMPv3, we also can specify the security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (DES), and encryption password.

Table 79–9 Configure the User

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Create the SNMP user	**snmp-server user** *user-name group-name* [**remote** *ip-address port-num*] **v3** [**auth** { **md5** | **sha** } *password* [**encrypt des** *password*]]	Mandatory

NOTE

- Configure the SNMPv3 user based on the user security model (USM), save the authentication and encryption information of each user. Note that only after configuring the authentication protocol, we can configure the encryption protocol.
- For the remote user (the so-called remote is relative to the local SNMPv3 entity. If the local SNMPv3 entity needs to communicate with other SNMPv3 entity, the other SNMPv3 entity is called remote SNMPv3 entity. This is mentioned in notify and proxy), we also need to specify the IP address and UDP port number of the remote user. When configuring the remote user, we should configure the engineID of the remote SNMP entity of the user first. Besides, each user should correspond with one group so that we can map one security model and security name to one group name via the view-based access control.
- When configuring the auto proxy forwarding and we may not know the IP address of the delegated device, we only need to input 0.0.0.0 at ip-address. Besides, the auto proxy forwarding should be combined with the keepalive mechanism.

Configure SNMP Notify

SNMPv3 notify configuration contains the following several kinds:

- SNMPv3 notify configuration: Configure the SNMPv3 notify and specify the type of the notify message as inform;
- SNMPv3 notify filter configuration: Notify filter means the filter used to determine whether one notify message should be sent to one destination address.
- SNMPv3 notify address map table configuration: Associate the notify address with one filter table.

Table 79–10 Configure the Notify

Step	Command	Description
Enter the global configuration mode	**config terminal**	-
Configure the SNMP notify	**snmp-server notify notify** *notify-name taglist* **inform**	Mandatory
Configure the SNMP notify filter	**snmp-server notify filter** *filter-name oid-subtree* { **exclude** | **include** }	Mandatory Exclude: Filter out the notifications of all objects in the MIB sub tree. Include: Inform all objects in the MIB sub tree.
Configure the SNMP address parameters	**snmp-server AddressParam** { *address-name* | **paramIn** } **v3** *user-name* { **noauth** | **authpriv** | **authnopriv** }	Mandatory
Configure the SNMP notify filter map table	**snmp-server notify profile** *filter-name address-param*	Mandatory *filter-name*: Specify the notify filter name to be mapped *address-param*: Specify the address parameter name to be mapped.

Configure SNMP Proxy Forwarding

If the network work station cannot directly access the managed SNMP proxy, the intermediate device needs to support the proxy forwarding. Currently, only SNMPv3 supports the proxy forwarding.

Table 79–11 Configure the Proxy Forwarding

Step	Command	Description
Enter the global configuration mode	**config terminal**	-

Step	Command	Description
Configure the SNMP remote engine ID	**snmp-server engineID remote** *ip-address port-num* [**vrf** *vrf-name*] *engine-id* [*group-name*]	Mandatory Configure the engine ID of the SNMP entity needing the proxy forwarding
Configure the SNMP address parameters	**snmp-server AddressParam** [*address-name* | **paramIn**] **v3** *user-name* { **noauth** | **authpriv** | **authnopriv** }	Mandatory
Configure the SNMP notify address	**snmp-server TargetAddress** *target-name ip-address port-num address-param taglist time-out retry-num*	Mandatory
Configure the SNMP proxy forwarding	**snmp-server proxy** *proxy-name* { **inform** | **trap** | **read** | **write** } { *engineId* | **auto** } *engineId address-param target-addr* [*context-name*]	Mandatory

79.2.4 Configure SNMP Trap *-B -S -E -A*

Trap is the information sent by SNMP agent to network workstation, used to report some specific events. Trap packets include general Traps and custom Traps. General Traps include Authentication, Linkdown, Linkup, Coldstart and Warmstart; custom Traps are output according to the requirements of each module.

Table 79-12 Configure Trap

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Traps enabling link interface down or up	**snmp-server enable traps snmp** [**linkup** | **linkdown**]	Required By default, SNMP Trap is not enabled
Enter the interface configuration mode	**interface** *interface-type interface-num*	Optional

Steps	Command	Description
Traps configuring interface state changes	**snmp trap link-status**	Optional
Configure the Trap target host	**snmp-server host {** *ip-address* | *host-name* **} traps {community** *community-name* **version { 1 | 2 } | user** *username* **authnopriv | authpriv | noauth version 3 }[port** *port-num* **| vrf** *vrf-name* **]**	Required Specify IP address as the IP address of the network workstation
Configure the source address of the Trap packet	**snmp-server trap-source** *ip-address*	Optional

NOTE

- In general, there will be a lot of Trap information occupying the Device resources and thus affecting the Device performance, it is recommended to enable the Trap function of the specified module as required, rather than all modules.

79.2.5 SNMP Monitoring and Maintaining *-B -S -E -A*

Table 79–13 SNMP Monitoring and Maintaining

Command	**Description**
show snmp-server	View the SNMP protocol packet statistics information
show snmp-server AddressParams	View the SNMP proxy address parameter information
show snmp-server community	View the SNMP proxy community information
show snmp-server contact	View the device manager contact
show snmp-server context	View the SNMPv3 context

Command	Description
show snmp-server engineGroup	Display the information of the SNMP proxy engine group
show snmp-server engineID	Display the information of the SNMP proxy engine ID
show snmp-server group	View the SNMP proxy user group information
show snmp-server Host	Display the information of the SNMP proxy trap host
show snmp-server location	View the location information of the device
show snmp-server notify filter	Display the information of the SNMP proxy notify filter
show snmp-server notify notify	Display the information of the SNMP proxy notify
show snmp-server notify profile	Display the associated information of the SNMP proxy notify
show snmp-server proxy	View the SNMP proxy forwarding information
show snmp-server reg-list	View the module information of the SNMP registered MIB
show snmp-server TargetAddress	View the SNMP proxy address entry information
show snmp-server user	View the SNMP user information
show snmp-server view	View the SNMP view information

79.3 SNMP Typical Configuration Example

79.3.1 Configure SNMP v1/v2c Proxy Server *-B -S -E -A*

Network Requirements

- Device is the SNMP Agent device and the route with the NMS server is reachable.
- NMS monitors and manages Device via SNMP v1 or SNMP v2c; when Device fails, it actively reports to NMS.

Network Topology

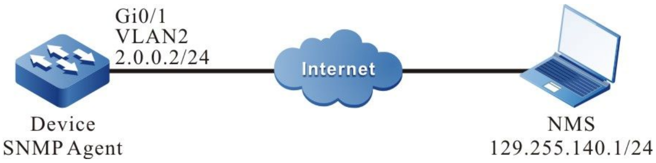


Figure 79-3 Networking of Configuring SNMP v1/v2c Proxy Server

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Enable the SNMP proxy on Device and configure the SNMP community name.

#Configure Device.

Enable the SNMP proxy; configure the node view name as default, read-only community name as public and read-write community name as public.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
Device(config)#snmp-server community public view default ro
Device(config)#snmp-server community public view default rw
```

Step 4: Configure Device to send the Trap packets to the network work station (NMS) actively and use the community name public.

#Configure Device.

```
Device(config)#snmp-server enable traps
Device(config)#snmp-server host 129.255.140.1 traps community public version 2
```

NOTE

- The SNMP version specified in the **snmp-server host** command should be consistent with the SNMP version running on NMS.

Step 5: Configure NMS.

#On the NMS using SNMP v1/v2c, we need to set “read-only community name” and “read-write community name”. Besides, we also need to set “timeout” and “re-try times”. The user queries and configures the device via the NMS.

NOTE

- When using the read-only community name, the user can only query the device via NMS.
- When using the read-write community name, the user can query and configure the device via NMS.

Step 6: Check the result.

#NMS can query and configure some parameters of Device via the MIB node. NMS can receive various Trap information from Device, such as interface up, down of Device, the route change caused by the network oscillation. Device generates the corresponding Trap information and sends to NMS.

79.3.2 Configure SNMP v3 Proxy Server *-B -S -E -A*

Network Requirements

- Device is the SNMP Agent device and the route with the NMS server is reachable.
- NMS manages Device via SNMPv3.

Network Topology

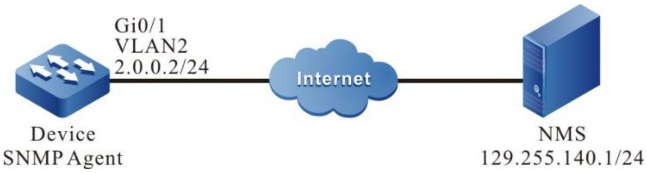


Figure 79-4 Networking of Configuring the SNMP v3 Proxy Server

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted).

Step 3: Enable the SNMP proxy on Device and configure the SNMPv3 basic information.

#Configure Device.

Enable the SNMP proxy; configure the node view name as default and it can access all objects in the node 1.3.6.1.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default1.3.6.1 include
```

Configure the user group as public and security level as authpriv; the read-write view and notify view both use default; configure the user name as public, belonging to the user group public, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES and encryption password as admin.

```
Device(config)#snmp-server group public v3 authpriv read default write default notify default
Device(config)#snmp-server user public public v3 auth md5 adminencrypt des admin
```

Configure the text name as public.

```
Device(config)#snmp-server context public
```

Step 4: Configure NMS.

#On the NMS using SNMP v3, we need to set the user name and select the security level. According to different security levels, we need to set the authentication algorithm, authentication password, encryption algorithm, encryption password and so on. Besides, we also need to set "timeout" and "re-try times". The user queries and configures the device via the NMS.

Step 5: Check the result.

# On NMS, we can query and set some parameters of Device via the MIB node.

79.3.3 Configure SNMP v3 trap Notice *-B -S -E -A*

Network Requirements

- Device is an SNMP Agent device and it can be routed with NMS server.
- NMS monitors Device through SNMP v3. In case of failure or error, Device will actively report the corresponding situation to NMS.

Network Topology

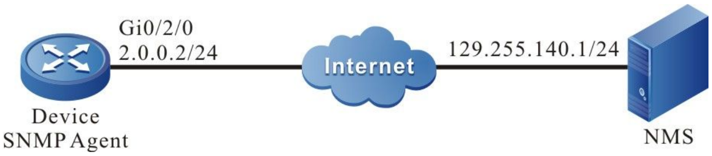


Figure 79-5 Configure SNMP v3 trap Notice Networking

Configuration Steps

Step 1: Configure IP addresses of the interfaces (omitted).

Step 2: Enable SNMP agency on Device and Configure the general information of SNMP v3.

#Configure Device.

Enable SNMP agency; configure the node view name to default, and all objects under node 1.3.6.1 to be accessible.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
```

Configure user group as public, security level as authpriv, read-write view and notify view as default; configure user name as public, belonging to user group public, authentication algorithm as MD5, authentication password as Admin, encryption algorithm as DES, and encryption password as Admin.

```
Device(config)#snmp-server group public v3 authpriv read default write default notify default
Device(config)#snmp-server user public public v3 auth md5 Admin encrypt des Admin
```

Configure Device to send all Trap information.

```
Device(config)#snmp-server enable traps
```

Step 3: Configure Device to send SNMP v3 trap packets to NMS.

#Configure Device.

Configure the user name of SNMP V3 trap on NSM as public and the security level as authpriv.

```
Device(config)#snmp-server host 129.255.140.1 version 3 user public authpriv
```

Step 4: Configure NMS.

#On NMS, configure the user name and password consistent with SNMP agency to run network management software and listen for UDP 162 port.

Step 5: Check the result.

#NMS can receive all kinds of Trap information from Device, such as up and down interfaces of Device, routing changes caused by network oscillations, etc., and Device will generate corresponding Trap information and send it to NMS.

79.3.4 Configure SNMP v3 Notify *-B -S -E -A*

Network Requirements

- Device is the SNMP Agent device and the route with the NMS server is reachable.
- NMS monitors Device via SNMPv3. When Device fails or has something wrong, it actively reports to NMS.

Network Topology

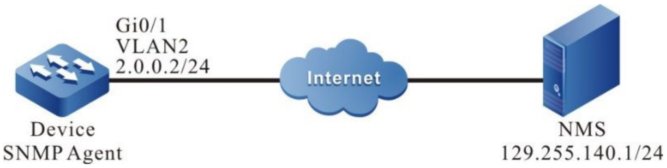


Figure 79-6 Networking of Configuring SNMPv3 Notify

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted).

Step 3: Enable the SNMP proxy on Device and configure the SNMPv3 basic information.

#Configure Device.

Enable the SNMP proxy; configure the node view name as default and it can access all objects in the node 1.3.6.1.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
```

Configure the user group as group1 and security level as authpriv; the read-write view and notify view both use default.

```
Device(config)#snmp-server group group1 v3 authpriv read default write default notify default
```

Configure the user group as user2, belonging to the user group group1, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES and encryption password as admin.

```
Device(config)#snmp-server user user2 group1 public v3 auth md5 admin encrypt des admin
```

Configure the text name as public.

```
Device(config)#snmp-server context public
```

Step 4: Configure Device to send notify message to NMS.

#Configure Device.

Configure the IP address and engineID of the remote user, that is, NMS.

```
Device(config)#snmp-server engineID remote 129.255.140.1 162 bb87654321
```

Configure the remote user name as user1, belonging to the user group group1, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES and encryption password as admin.

```
Device(config)#snmp-server user user1 group1 remote 129.255.140.1 162 v3 auth md5 adminencrypt des admin
```

Configure the local address parameter name as param-user1; configure the target address name as target-user1; use the address parameter param-user1; the target address list name is target-user1.

```
Device(config)#snmp-server AddressParam param-user1 v3 user1  authpriv
Device(config)#snmp-server TargetAddress target-user1  129.255.140.1 162 param-user1 tag-user1 10 3
```

Configure the notify entity as notify-user1; configure the filter entity of notify as filter-user1, containing the notify of all objects in the node 1.3.6.1; configure the notify configuration table, and let the filter entity fileter-user1 associate with the address parameter param-user1.

```
Device(config)#snmp-server notify notify notify-user1 tag-user1  inform
Device(config)#snmp-server notify filter filter-user1 1.3.6.1 include
Device(config)#snmp-server notify profile filter-user1 param-user1
```

Step 5: Configure NMS.

#On NMS, do not need to configure, but just need to run the network management software and monitor the UDP port 162.

Step 6: Check the result.

#NMS can receive various Trap information from Device, such as interface up, down of Device, the route change caused by the network oscillation. Device generates the corresponding Trap information and sends to NMS.

79.3.5 Configure SNMP v3 Proxy Forwarding *-B -S -E -A*

Network Requirements

- The route from Device2 to NMS server is reachable.
- Device2 is the proxy device Agent; Device1 is the delegated device.
- On Device1 and Device2, run SNMPv3.
- On NMS, run SNMPv3. NMS manages Device1 and Device2 via SNMP v3.

Network Topology

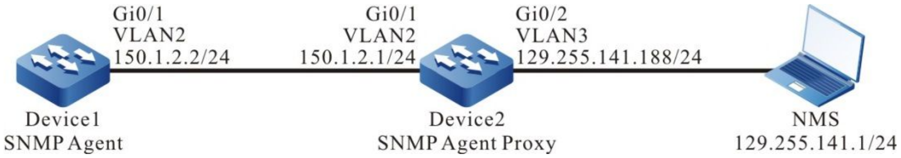


Figure 79-7 Networking of Configuring the SNMP v3 Proxy Forwarding

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted).

Step 3: On the proxy device Device2, enable the SNMP proxy and configure the SNMPv3 basic information.

#Configure Device2.

Enable the SNMP proxy; configure the node view name as default and it can access all objects in the node 1.3.6.1.

```
Device2#configure terminal
Device2(config)#snmp-server start
Device1(config)#snmp-server view default 1.3.6.1 include
```

Configure the user group as group-local and security level as noauth; the read-write view and notify view both use default; configure the user name as user1, belonging to the user group group-local, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES and encryption password as admin.

```
Device2(config)#snmp-server group group-local v3 noauth read default write default notify default
Device2(config)#snmp-server user user1 group-local v3 auth md5 admin encrypt des admin
```

Step 4: On the delegated device Device1, enable the SNMP proxy and configure the SNMP view.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#snmp-server start
Device1(config)#snmp-server view default 1.3.6.1 include
```

Step 5: Configure the information of the delegated device on the proxy device Device2.

#Configure Device2.

Configure the IP address and engineID of the delegated device.

```
Device2(config)#snmp-server engineID remote 150.1.2.2 161 800016130300017a000137
```

Configure the user group of the delegated device as group-user, security level as authpriv; both the read-view and notify view use default.

```
Device2(config)#snmp-server group group-user v3 authpriv read default write default notify default
```

Configure the user name as re-user, belonging to the user group group-user, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES and encryption password as admin.

```
Device2(config)#snmp-server user re-user group-user remote 150.1.2.2 161 v3 auth md5 admin encrypt des
admin
```

Configure the local address parameter name as plocal and remote address parameter name as puser; configure the target address name as tuser and use the address parameter puser.

```
Device2(config)#snmp-server AddressParam plocal v3 user1 authpriv
Device2(config)#snmp-server AddressParam puser v3 re-user authpriv
Device2(config)#snmp-server TargetAddress tuser 150.1.2.2 161 puser taguser 10 2
```

Configure the proxy forwarding name as proxy-re-user, the operation authority as WRITE, the engineID of the delegated device as 800016130300017a000137, the used address parameter plocal, the used target address tuser; configure the context name as proxyuser.

```
Device2(config)#snmp-server proxy proxy-re-user WRITE 800016130300017a000137 plocal tuser proxyuser
Device2(config)#snmp-server context proxyuser
```

#View the engineID information of Device2.

```
Device2#show snmp-server engineID
Local  engine ID: 80001613030000000052fd
IPAddress: 150.1.2.2.0.161 remote engine ID: 800016130300017a000137
```

NOTE

- The engineID of the remote device should be consistent with the delegated device. The engineID of the device can be viewed via the **show snmp-server engineID** command.
- The monitoring protocol of the delegated device is UDP and the port is 161.

Step 6: Perform the related configuration of SNMPv3 on the delegated device Device1.

#Configure Device1.

Configure the user group as g1 and security level as authpriv; the read-write view and notify view both use default; configure the user name as re-user, authentication algorithm as MD5, authentication password as admin, encryption algorithm as DES and encryption password as admin.

```
Device1(config)#snmp-server group g1 v3 authpriv read default write default notify default
Device1(config)#snmp-server user re-user g1 v3 auth md5 admin encrypt des admin
Device1(config)#snmp-server context proxyuser
```

Step 7: Configure NMS.

#SNMP v3 adopts the authentication and encryption security mechanism. On the NMS, we need to set the user name and select the security level. According to different security levels, we need to set the authentication algorithm, authentication password, encryption algorithm, encryption password and so on. Besides, we also need to set “timeout” and “re-try times”. The user can query and configure the device via the NMS. When it is necessary to query or configure the delegated device, we also need to set the engineID of the proxy forwarding as the engineID of the delegated device on NMS.

Step 8: Check the result.

#On NMS, we can query and set some parameters of Device2 and Device1 via the MIB node.

80 RMON

80.1 Overview

One important function of the network management is to monitor the element performances of the network. In the traditional SNMP network management mode, the initiative of the management is mainly mastered by the network management station. Usually, the network management work station regularly polls the data of the device and then measures and analyzes in the network management system, so as to get the desired information of the administrator. In this mode, the network management work station needs to send and receive lots of packets to the network devices. When there are many devices in the network, it causes the additional load for the network. Meanwhile, the network blocking and other factors take various accidents to the running of the network management system. As for this, we put forward the RMON (Remote Network Monitoring) concept.

The realizing of RMON still needs the supporting of the SNMP protocol. In fact, it is one group of MIBs, distributed in MIB-2, and the object ID is 1.3.6.1.2.1.16. Compared with other general MIB, RMON adds the calculation at Agent during realizing, that is, put the processing, such as performance statistics in the device. This realizes the distributed processing in the whole network, reducing the disadvantages brought by the polling of the network management work station.

RMON needs to realize lots of calculation functions, so the previous RMON proxy (also called Probe) is acted by a special device, distributed in the network to monitor the corresponding target. With the improvement of the processing capability of the network device, RMON is gradually integrated to the network devices, so as to realize the RMON requirement high-efficiently. However, this also puts forward higher performance requirement for the network devices. After all, the calculations of RMON occupy lots of system resources, reducing the system performance. This is also the additional cost brought by the management, so RMON is mainly realized in the hardware with the network processing capability, such as switching chip.

RMON MIB has 10 groups:

- statistics: Measure all Ethernet interfaces of the device, such as broadcast and conflict;
- history: Record the samples of the periodical statistics information that is taken out from the statistics group;
- alarm: Permit the administration Console user to configure the sampling interval and alarm when the values of any counters or integers (recorded by the RMON proxy) exceed the threshold value;
- host: Include the input/output traffics of various types of hosts adhering to the subnet;
- hostTopN: Contain the stored statistics information of hosts, some parameters in the host tables of these hosts are the highest;
- matrix: Indicate the error and utilization information in the form of matrix, so that the

operator can use any address pair to search for information;

- filter: Permit the monitor to monitor the packets matched with the filter;
- event: Present the table of all events generated by the RMON proxy;
- tokenRing: Maintain the statistic and configuration information of a subnet which is a token ring

80.2 RMON Function Configuration

Table 80-1 RMON Function Configuration List

Configuration Task	
Enable the RMON function	Enable the RMON function
Configure the RMON alarm group	Configure the RMON alarm instance
Configure the RMON event group	Configure the RMON trigger event
Configure the RMON history group	Configure the RMON history group instance
Configure the RMON statistics group	Configure the RMON statistics management function

80.2.1 Enable RMON Function *-B -S -E -A*

Configuration Conditions

None

Enable RMON Function

Enabling RMON is to provide the related resource for the RMON monitoring function. The sources can take effect only after configuring the RMON monitoring group function.

Table 80-2 Enable the RMON Function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-

Step	Command	Description
Enable the RMON function	**rmon**	Mandatory

80.2.2 Configure RMON Alarm Group *-B -S -E -A*

RMON alarm group function means to configure multiple alarms and each alarm monitors one alarm instance. Within the sampling interval, when the alarm instance data value changes and exceeds the increasing threshold or the decreasing threshold, trigger the alarm event. According to the processing mode defined by the alarm event group, process the alarms. When the data value exceeds the threshold continuously, alarm only for the first exceeding.

Configuration Conditions

Before configuring the RMON alarm group, first complete the following task:

- Enable the SNMP proxy function
- Enable the TRAP function of RMON in SNMP

Configure RMON Alarm Instance

Table 80-3 Configure the RMON Alarm Instance

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Optional
Configure the RMON alarm group	**rmon alarm** *alarm-num OID interval* { **absolute | delta** } **risingthreshold** *rising-threshold* [*rising-event*] **fallingthreshold** *falling-threshold* [*falling-event*] [**owner** *owner*]	Mandatory By default, the alarm trigger event group is 1. By default, the owner of the alarm group is config.

80.2.3 Configure RMON Extended Alarm Group *-B -S -E -A*

RMON extended alarm group can calculate the alarm variables, and then compare the calculated results with the set threshold to achieve more abundant alarm functions.

Configuration Conditionss

Before configuring the RMON alarm group, first complete the following task:

- Enable SNMP agent function;
- Enable RMON TRAP function in SNMP.
- Configure a statistics group

Configure RMON Alarm Instance

Table 80-4 Configure the RMON Alarm Instance

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enable RMON functions	**rmon**	Optional
Configure the statistics group	**rmon statistics ethernet** *statistics-num OID* [**owner** *owner*]	Required By default, the owner of the statistics group is config.
Configure the RMON alarm group	**rmon prialarm** *alarm-num WORD interval* { **absolute** | **delta** } **risingthreshold** *rising-threshold rising-event* **fallingthreshold** *falling-threshold falling-event* **entrytype forever** [**owner***owner*]	Required By default, the owner of the alarm group is config.

80.2.4 Configure RMON Event Group *-B -S -E -A*

Configuring the RMON event group function means to configure multiple events, defining the event serial number and processing mode of each event. The event has the following several processing modes: The event is recorded in the log; the event sends the TRAP message to the network management system; record the event in the log and send the TRAP message to the network management system, but do not process.

Configuration Conditions

Before configuring the RMON event group, first complete the following task:

- Enable the SNMP proxy function
- Enable the TRAP function of RMON in SNMP

Configure RMON Trigger Event

RMON trigger event is mainly used to process the events when the RMON alarm happens.

Table 80-5 Configure the RMON Trigger Event

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Optional
Configure the RMON event group	**rmon event** *event-num* [**description** *event-description* / **log** *max-num* / **owner** *owner* / **trap** *communit*]	Mandatory By default, the owner of the event group is config.

80.2.5 Configure RMON History Event *-B -S -E -A*

Configuring RMON history group function means to configure multiple history groups. RMON history group stores the subnet data got by sampling with fixed interval. The group comprises the history control table and history data. The control table defines the sampled subnet interface serial number, the sampling interval, and hot much data to sample each time, while the data table is used to store the data got during the sampling.

Configuration Conditions

Before configuring the RMON history group, first complete the following task:

- Enable the SNMP proxy function

Configure RMON History Group Instance

RMON history group mainly configures the monitor object of the history control table, sampling interval, hot much data to sample, and so on.

Table 80-6 Configure the RMON History Group Instance

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Optional
Configure the RMON history group	**rmon history control** *history-num OID buckets-num* [**interval** *interval*] [**owner** *owner*]	Mandatory By default, the sampling interval is 1800s. By default, the owner of the history group is config.

80.2.6 Configure RMON Statistics Group *-B -S -E -A*

Configuring the RMON statistics group function is to configure the monitor object as the statistics information of the Ethernet interface. The statistics group provides one table and each row of the table indicates the statistics information of one subnet. The network administrator can get various statistics information of one segment from the table (the traffic of one segment, the distributing of various types of packets, various types of error packets, and the number of collisions and so on).

Configuration Conditions

Before configuring the RMON statistics group, first complete the following task:

- Enable the RMON function
- Enable the SNMP proxy function

Configure Statistics Management Function

Table 80-7 Configure RMON Statistics Management Function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable the RMON function	**rmon**	Mandatory
Configure the RMON statistics group	**rmon statistics ethernet** *statistics-num OID* [**owner** *owner*]	Mandatory

Step	Command	Description
		By default, the owner of the statistics group is config.

80.2.7 RMON Monitoring and Maintaining *-B -S -E -A*

Table 80-8 RMON Monitoring and Maintaining

Command	Description
show rmon alarm	Display the RMON alarms configured in the device
show rmon alarm supportVariable	Display the monitor objects supported in the device
show rmon event	Display the RMON event configured in the device
show rmon history { **control** | **ethernet** *control-num* }	Display the RMON history group configured in the device
show rmon statistics ethernet	Display the RMON statistics group configured in the device

80.3 RMON Typical Configuration Example

80.3.1 Configure RMON Basic Functions *-B -S -E -A*

Network Requirements

- Device is the RMON proxy device and the route with the NMS server is reachable;
- Monitor and manage the event groups, alarm groups, history groups and statistics groups of RMON via NMS.

Network Topology

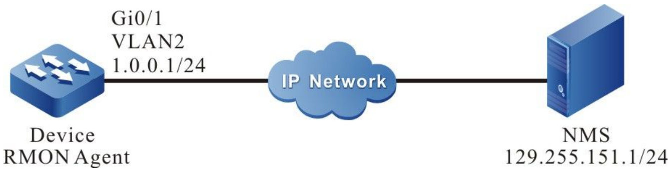


Figure 80-1 Networking of Configuring the RMON Basic Functions

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (Omitted)

Step 2: Configure the IP address of the interface. (Omitted)

Step 3: Configure the SNMP proxy.

#Enable the SNMP proxy, and configure the node view node as default and read-only community name as public.

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
Device(config)#snmp-server community public view default ro
```

#Enable the SNMP Trap function and configure the destination address and the used community name of the Trap packet.

```
Device(config)#snmp-server enable traps
Device(config)#snmp-server host 129.255.151.1 traps community public
```

Step 4: Configure the RMON event group, alarm group, history group and statistics group of Device.

#Enable the RMON proxy.

```
Device(config)#rmon
```

#Configure the serial number of the event group as 1 and record the ingress packets of port gigabitethernet0/1.

```
Device(config)#rmon event 1 description gigabitethernet0/1_in_octes log 100 trap public
```

#Configure the alarm event group; the monitor object is ifInOctets.1; configure the sampling of the relative value; the sampling interval is 10s. Configure the increasing and decreasing threshold as 100; configure the triggered event of reaching the threshold value as event1.

```
Device(config)#rmon alarm 1 ifInOctets.1 10 delta risingthreshold 100 1 fallingthreshold 100 1 owner 1
```

#Configure the RMON statistics group.

```
Device(config)#rmon statistics ethernet 1 ifIndex.1
```

#Configure the RMON history group.

```
Device(config)#rmon history control 1 ifIndex.1 10
```

NOTE

- The corresponding port of the instance index ifInOctets.1 is gigabitethernet0/1 on the device.

- The remote monitored object instance index needs to be read from the interface table ifEntry of MIB-2.

Step 5: Configure NMS.

#On NMS using SNMP v1/v2c, we need to set “Read-only community name”, “timeout” and “Retry times”.

Step 6: Check the result.

#View the RMON event group entry configuration of Device.

```
Device#sh rmon event
Event 1 is active, owned by config
Description : gigabitethernet_0/1_in_octes
Event firing causes: log and trap, last fired at 11:38:07

Current log entries:
      logIndex         logTime           Description
-----------------------------------------------------------------
          1            11:38:07       gigabitethernet_0/1_in_octes
```

#Configure the RMON alarm entry configuration of Device.

```
Device#show rmon alarm
Alarm 1 is active, owned by 1
Monitoring variable: ifInOctets.1,      Sample interval: 10 second(s)
Taking samples type: delta,     last value was 4225
Rising threshold :   100,       assigned to event: 1
Falling threshold :  100,       assigned to event: 1
```

#Configure RMON statistics group entry configuration of Device.

```
Device#sh rmon statistics ethernet
-------------------------------
Ethernet statistics table information:
        Index: 1
        Data Source: ifIndex.1
        Owner: config
        Status: Valid
------------------------------
 ifIndex.1 statistics information:
------------------------------
 DropEvents:0
 Octets: 26962295
 Pkts:252941
 BroadcastPkts:156943
 MulticastPkts:62331
 CRCAlignErrors:51
 UndersizePkts:0
 OversizePkts:0
 Fragments:0
 Jabbers:0
 Collisions:0
 Pkts64Octets:167737
 Pkts65to127Octets:47962
 Pkts128to255Octets:22497
 Pkts256to511Octets:9967
 Pkts512to1023Octets:4032
 Pkts1024to1518Octets:745
```

#View the RMON history group entry configuration of Device.

```
Device#sh rmon history control
----------------------------------
RMON history control entry index: 1
        Data source: IfIndex.1
        Buckets request: 10
        Buckets granted: 2
        Interval: 1800
        Owner: config
        Entry status: Valid
----------------------------------
```

#NMS can query the History, Event and Statistics information in Device via MIB.

NMS can receive the Trap information of the Alarm event from Device. For example, when the ingress traffic change rate of the monitor interface is larger than the increasing threshold or smaller than the decreasing threshold, Device generates the corresponding Trap information and sends to NMS.

81 Virtualization

81.1 Virtualization Overview

In consideration of that users' requirements for low cost and high reliability are constantly on the rise, our company has proposed a technology for combining multiple physical switches to form a virtual switch. The technology is called “virtualization”.

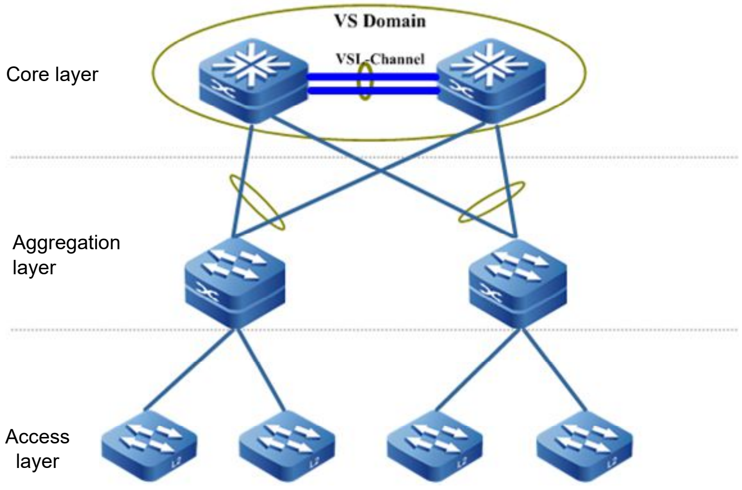


Figure 81-1 Virtualization Physical Network View

As shown in Figure 1-1, the two devices at kernel layer are connected via a virtualization link interface to form a VS Domain (also referred to as the stacking system), the devices at aggregation layer are uplinked to the VS Domain via link rendezvous. For other network devices, the kernel layer's VS Domain is a virtual device.

Compared with conventional L2 STP and L3 VRRP/VBRP technology, this technology has the following merits:

- Multiplication and efficient use of bandwidth

In conventional technology solutions, one of the two original up-links is in forwarding status while the other is in back-up status due to the operation of STP/RSTP/MSTP. With virtual switching technology, however, multiple devices can be considered as a logic device. As a result, it is no longer necessary to block some links and the two up-links can form a link-aggregation group for forwarding data. Thus, the bandwidth of these links is efficiently exploited without wasting the bandwidth resource. Furthermore, a cross-device and cross-board aggregation link can provide a redundant link and realize dynamic load balancing for efficient use of all available bandwidth.

- High reliability

The virtual switching system consists of multiple pieces of member devices. Master control device (master controller) is responsible for the operation, management and maintenance of the entire virtual switch system. Other member devices are in backup state. When the master controller malfunctions, the system will, instead of relying on the convergence of STP/RSTP/MSTP, VRRP/VBRP protocols, promptly elect a new master controller from other member devices in backup state. Thus, the virtual switching system's business will not be interrupted, thereby improving the system's reliability.

- Simplified network topology

A virtual device formed by the virtualization technology is equivalent to a Device in the network. The device is connected to peripheral devices via the aggregation link. Since the system is free of L2 loop, it is not necessary to configure STP/RSTP/MSTP protocol. A variety of control protocols run on the virtual device, reducing numerous message interactions between devices and routing convergence time.

- Centralized management

When two or more devices form a stacking system, the member devices' control plane in the virtual switching system is in backup state but their data plane is active. Users can log on to the virtual switch system via the port of any member device to centralizedly manage the entire virtual device without having to access each member device for management separately.

81.1.1 Basic Concepts

VS Domain

VS Domain consists of one or more pieces of member devices. The domain IDs of member devices in the same VS Domains must be configured to the same value. Domain ID is the only parameter that determines a VS Domain. As the VS Domain's MAC address is acquired in virtual MAC address mode, the VS Domain's ID is the only parameter that determines the MAC address. Therefore, multiple stacking systems cannot have the same domain ID in the same LAN.

Virtualization Member Device

Every physical device in VS Domain is also referred to as a virtualization member device. In the same stacking domain, member ID is the only parameter that determines a member device.

Virtualization Link Interface and Its Member Ports

A virtualization link interface is formed by bundling together multiple physical ports with stacking capabilities. A virtualization link interface is a logic link channel for internal protocol message exchange and transaction data forwarding between member devices in the stacking system. All physical ports in the virtualization link interface are known as its member ports.

The member devices join in the same virtual switching domain and interconnect via the virtualization link interface to form a virtual device.

LMP

LMP (Link Manage Protocol) is used for the management of virtualization link interface and its member ports.

RRP

RRP (Role Resolution Protocol) is used for the election of member device role in a stacking system.

TDP

TDP (Topology Discovery Protocol) is used for advertising member device information in a stacking system, in order to ensure the consistency of all member device information in the stacking system.

81.2 Configuration of Virtualization Function

Table 81-1 Functional Configuration List of Virtualization

Configuration task	
Configure virtualization member device	Configure virtualization member device domain ID
	Configure virtualization member device ID
	Configure virtualization member device's priority level
Configure virtualization link interface	Create virtualization link interface
	Configure interface to join in virtualization link interface
Configure device operation mode	Configure device operation mode

81.2.1 Configure Virtualization Member Device *-B -S -E -A*

A Device can be configured before and after its joining in the virtual switch stacking domain, including changing its member ID, domain ID, and/or priority level.

NOTE

- In stacking mode, when virtualization member device's member ID or domain ID is changed, the newly configured member ID or domain ID will not take effect immediately. Instead, the corresponding configuration will take effect only after the corresponding virtualization member devices have saved the configurations and restarted.

Configuration Conditions

None

Configure Virtualization Member Device Domain ID

Table 81-2 Configure Virtualization Member Device Domain ID

Steps	Command	Description
Enter virtualization member configuration mode	**switch virtual member** *member-id*	-
Configure virtualization member device domain ID	**domain** *domain-id*	Required By default, virtualization member device domain ID is 100

NOTE

- In stacking mode, when adding virtualization member devices to VS Domain, make sure the virtualization member devices' domain ID is identical, otherwise, the virtualization member devices will not be able to join in the same VS Domain.
- In stacking mode, when domain ID is changed, the new domain ID will not immediately take effect; instead, the new domain ID will take effect only after the virtualization member device has saved the configuration and restarted.

Configure Virtualization Member Device ID

Configure virtualization member device ID in response to two circumstances: 1) configure the virtualization member device ID for a virtualization member device that has never been configured that ID before; 2) change the virtualization member device ID of a virtualization member device that has been configured that ID to a new ID. There are two commands relating to virtualization member device ID, one is for configuring virtualization member device ID, the other is for changing virtualization member device ID, as shown in Table 1-3.

Table 81-3 Configure Virtualization Member Device ID

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure virtualization member device ID	**switch virtual member** *member-id*	Required By default, device has no virtualization member device ID
Change virtualization member device ID	**switch virtual member** *member-id* **rename** *member-id-new*	Optional

NOTE

- In stacking mode, after virtualization member device ID is changed, the configuration has to be saved and the system has to be restarted for the new virtualization member device ID to take effect.
- In a VS Domain, every virtualization member device has a unique member ID. No two virtualization member devices can have identical same member, otherwise, the virtualization member devices cannot stack normally.

Configure Virtualization Member Device's Priority Level

When multiple virtualization member devices join in the same VS Domain, the possibility of that a virtualization member device is elected as master controller can be increased by configuring the priority level of all virtualization member devices. The greater the priority number, the higher the priority level.

Table 81-4 Configure Virtualization Member Device's Priority Level

Steps	Command	Description
Enter virtualization member configuration mode	**switch virtual member** *member-id*	-
Configure virtualization member device's priority level	**priority** *priority-num*	Required By default, the priority level of virtualization member device is 100

NOTE

- Rules for election of virtualization master controller in VS Domain:
  1. Virtualization master controller have higher priority; if there are multiple virtualization master controllers, a second comparison should be carried out; if there is no virtualization master controller, a third comparison should be carried out; otherwise, the comparison should end.
  2. A Device that runs as virtualization master controller for longer duration should have higher priority; if more than one master controllers have identical operation duration, a third comparison should be carried out, otherwise, the comparison should end.
  3. A Device that has higher priority level should take precedence; if more than one device have identical priority level, a fourth comparison should be carried out, otherwise, the comparison should end.
  4. A Device with smaller member ID has higher priority.

81.2.2 Configure Virtualization Link Interface *-B -S -E -A*

A virtualization link interface is a logical interface. It binds multiple physical ports that support stacking for centralizedly management of these physical ports. Any operation to the virtualization link interface applies to every physical member ports of the channel.

Configuration Conditions

None

Create Virtualization Link Interface

Table 81-5 Create Virtualization Link Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create virtualization link interface	**vsl-channel** *vsl-channel-id*	Required In standalone mode, vsl-channel-id is a one-dimensional value representing the virtualization link interface's ID; in stacking mode, it is a two-dimensional value, the first dimension of which

Steps	Command	Description
		is the virtual member switch's ID, the second dimension is the virtualization link interface's ID

NOTE

- When a virtualization link interface is deleted, all member ports in the virtualization link interface will exit the virtualization link interface, and all configurations of member ports will be restored to default settings. Before deleting a virtualization link interface, please make sure no loop will form in the network after the deletion.

Configure Interface to Join in Virtualization Link Interface

Table 81-6 Configure Interface to Join in Virtualization Link Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2 ethernet interface configuration mode	**interface** *interface-name*	-
Configure interface to join in virtualization link interface	**vsl-channel** *vsl-channel-id* **mode on** [**type extern**]	Required

NOTE

- All member ports in a virtualization link interface and their port capacity have to be identical.

81.2.3 Configure Device Operation Mode *-B -S -E -A*

Current device supports two operation modes, standalone mode and stacking mode. The device can form a VS Domain with other virtualization member devices only when it runs in stacking mode.

Configuration Conditions

None

Configure device operation mode

Table 81-7 Configure Device Operation Mode

Steps	Command	Description
Enter privilege user mode	**enable**	-
Configure device operation mode	**switch mode** { **stand-alone** | **virtual** }	Required By default, device runs in standalone mode

NOTE

- When the operation mode of the Device is changed, the Device will be restarted and after the restart will run in the newly configured mode.
- Different operation modes of a Device correspond to their respective start configuration files.
- Before switching a Device into stacking mode, make sure it has been configured a virtualization member device ID, otherwise, the switchover will not be done.

81.2.4 Virtualization Monitoring and Maintaining *-B -S -E -A*

Table 81-8 Virtualization Monitoring and Maintaining

Command	Description
show switch virtual	Display VS Domain's basic information
show switch virtual local config	Display local virtualization member device's basic configuration information
show switch virtual local current	Display local virtualization member device's basic operation information
show switch virtual member *member-id* [**config** | **current**]	Display virtualization member device's basic information

Command	Description
show switch virtual topo	Display information on local virtualization member devices' forwarding paths to other virtualization member devices in the VS Domain
show switch vsl-channel [*vsl-channel-id*]	Display the information of virtualization link interfaces in VS Domain

81.3 Example of Virtualization Typical Configuration

81.3.1 Configure Devices to Form a Chain Stacking System *-B -S -E -A*

Network Requirements

- Make Device0, Device1 form a chain stacking system, in which Device0 is the master controller.

Network Topology

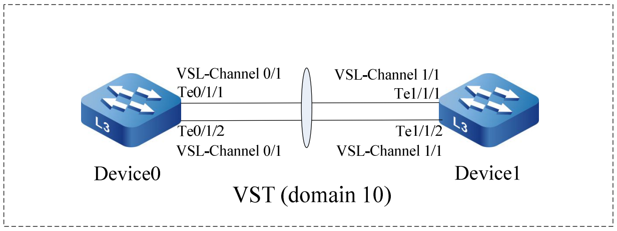


Figure 81-2 Configure Devices to Form a Chain Stacking System

Configuration Steps

Step 1: Configure Device0.

#On Device0, configure virtualization member device ID to 0, and configure domain ID to 10, priority level to 255.

```
Device0#configure terminal
Device0(config)#switch virtual member 0
Do you want to modify member id(Yes|No)?y
% Member ID 0 config will take effect only after the exec command 'switch mode virtual' is issued
Device0(config-vst-member-0)#domain 10
```

```
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device0(config-vst-member-0)#priority 255
Device0(config-vst-member-0)#exit
```

#On Device0, create virtualization link interface 1, and add port tengigabitethernet1/1 and tengigabitethernet1/2 to virtualization link interface 1.

```
Device0(config)#vsl-channel 1
Device0(config-vsl-channel-1)#exit
Device0(config)#interface tengigabitethernet 1/1-1/2
Device0(config-if-range)#vsl-channel 1 mode on
Device0(config-if-range)#exit
```

#On Device0, save the configuration.

```
Device0#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

Step 2: Configure Device1.

#On Device1, configure virtualization member device ID to 1, and configure domain ID to 10, priority level to 200.

```
Device1#configure terminal
Device1(config)#switch virtual member 1
Do you want to modify member id(Yes|No)?y
% Member ID 1 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#priority 200
Device1(config-vst-member-1)#exit
```

#On Device1, create virtualization link interface 1, and add port tengigabitethernet1/1 and tengigabitethernet1/2 to virtualization link interface 1.

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tengigabitethernet 1/1-1/2
Device1(config-if-range)#vsl-channel 1 mode on
Device1(config-if-range)#exit
```

#On Device1, save the configuration.

```
Device1#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

Step 3: Configure Device0, Device1 to operate in stacking mode.

#Configure Device0 to operate in stacking mode.

```
Device0#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-
number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
 ok
Reset system!
Jul 30 2014 17:36:14: %SYS-5-RELOAD: Reload requested
```

#Configure Device1 to operate in stacking mode.

```
Device1#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
 ok
Reset system!
Jul 30 2014 17:36:20: %SYS-5-RELOAD: Reload requested
```

Step 4: Check the result.

#Check on Device0, a chain stacking system has already been formed, and Device0 is the master controller.

```
Device0#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode        : VIRTUAL
Virtual Switch DomainId    : 10
Virtual Switch mac-address : 0001.7a6a.001b

--------------- VST MEMBER INFORMATION ------------------
CODE MemberID Role   Pri  LocalVsl        RemoteVsl
---- -------- ------ ---- --------------- ---------------
L    0        Master 255  vsl-channel 0/1 vsl-channel 1/1

     1        Member 200  vsl-channel 1/1 vsl-channel 0/1
```

82 MAD

82.1 MAD Overview

When the virtualization link interface in a stacking system malfunctions, the stacking system will split into multiple VS Domains, giving rise to multiple virtualization master controllers (hereinafter referred to as master controllers) of identical global configuration. Such situation is called multi-active. Since the split off logic devices have global configuration completely identical to the original logical device's, there will be network configuration conflict, leading to abnormal network traffic. In order to prevent such situation's impact on business, MAD (Multi-Active Detection) was invented.

Currently this stacking system supports two MAD modes, i.e., MAD LACP, and MAD Fast-Hello, which can meet different networking requirements.

There are two MAD statuses: Active and Recovery. Active means normal operation state, Recovery means disabled state. In disabled state, all L2/L3 ethernet interfaces and VLAN interfaces other than the virtualization link member ports and reserved interfaces will be turned off by MAD.

When receiving MAD detection messages, device will compare the data in the message and those of the logical device. If the VS Domain ID (sender's VS Domain ID) is identical to the logical device’s, and the Master ID (master controller's member ID in sender's VS Domain) in the message is different from the logical device’s, it is deemed that there is multi-active and multi-active election should be started. According to applicable election rules, in the same VS Domain, only one logical device can remain in Active status, other logical devices will enter Recovery status.

During MAD LACP networking, intermediate devices have to be used; during MAD Fast-Hello networking, intermediate devices can be used; or the devices can be directly connected. If direct connection mode is used, make sure that between any two virtualization member devices there is directly connected line for Multi-Active Detection (MAD). In other words, full connections have to be ensured.

82.2 Configuration of MAD Function

Table 82-1 Functional Configuration List of MAD

Configuration task	
Configure MAD LACP function	Configure MAD LACP function

Configuration task	
Configure MAD Fast-Hello function	Configure MAD Fast-Hello function
Configure reserved interface	Configure reserved interface
Configure recovery MAD status to Active	Configure recovery MAD status to Active

82.2.1 Configure MAD LACP Function *-B -S -E -A*

MAD LACP Multi-Active Detection (MAD) is for implementing Multi-Active Detection (MAD) and election by extending LACP protocol message field.

Configuration Conditions

None

Configure MAD LACP function

Table 82-2 Configure MAD LACP Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Create dynamic aggregation group	**link-aggregation** *link-aggregation-id* **mode lacp**	Required By default, no aggregation group has been created and designated
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	-
Enable MAD LACP function	**mad enable**	Required By default, MAD LACP function is not enabled

NOTE

- Only dynamic aggregation group supports the enabling of MAD LACP function.
- The intermediate devices used during networking must be our company's devices

Steps	Command	Description
that support LACP message pass through transmission.		

82.2.2 Configure MAD Fast-Hello Function *-B -S -E -A*

These protocol messages for MAD Fast-Hello Multi-Active Detection are defined by our company, they directly carry the data needed for Multi-Active Detection (MAD) and election.

Configuration Conditions

None

Configure MAD Fast-Hello function

Table 82-3 Configure MAD Fast-Hello Function

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure the transmission cycle of MAD Fast-Hello message in normal mode	**mad fast-hello normal interval** *interval-time*	Optional By default, the transmission cycle of MAD Fast-Hello message in normal mode is 2000 millisecond
Configure the transmission cycle of MAD Fast-Hello message in aggressive mode	**mad fast-hello aggressive interval** *interval-time*	Optional By default, the transmission cycle of MAD Fast-Hello message in aggressive mode is 500 millisecond
Configure aggressive mode duration	**mad fast-hello aggressive duration** *duration-time*	Optional By default, aggressive mode duration is 120 seconds
Enter VLAN configuration mode	**vlan** *vlan-id*	-

Steps	Command	Description
Configure control VLAN	**mad fast-hello control-vlan**	Required By default, control VLAN is not configured
Enter global configuration mode	**exit**	-
Enter L2 ethernet interface configuration mode	**interface** *interface-name*	-
Configure the port's link type to Trunk	**switchport mode trunk**	Required By default, port link type is Access
Turn off the port's STP function	**no spanning-tree enable**	Required By default, the port has been enabled the STP function
Configure control port	**mad fast-hello vlan** *vlan-id*	Required By default, control port is not configured

NOTE

- The control VLAN and control port of MAD Fast-Hello can only be used for MAD Fast-Hello and cannot be sued for configuring other businesses.
- STP function has to be turned off on the control port of MAD Fast-Hello.

82.2.3 Configure Reserved Interface *-B -S -E -A*

When MAD status changes to Recovery, the reserved interfaces will not be turned off by MAD. It is acceptable to configure ports and interfaces (e.g., management interfaces) that have to be maintained in UP state for special purposes as reserved ports/interfaces.

Configuration Conditions

None

Configure Reserved Interface

Table 82-4 Configure Reserved Interface

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Enter L2/L3 ethernet interface configuration mode	**interface** *interface-name*	Must be chosen alternatively Once in L2/L3 ethernet interface configuration mode, subsequent configurations only apply to current interfaces; in aggregation group configuration mode, subsequent configurations only apply to aggregation group; in interface configuration mode, subsequent configurations only apply to current interfaces.
Enter aggregation group configuration mode	**link-aggregation** *link-aggregation-id*	
Enter the interface configuration mode	**interface vlan** *vlan-id*	
Configure reserved interface	**mad exclude recovery**	Required By default, no reserved interface is configured

NOTE

- An aggregation group that has MAD LACP function enabled cannot be configured as reserved interface.

82.2.4 Configure Recovery MAD Status to Active *-B -S -E -A*

Configuration Conditions

None

Configure Recovery MAD Status to Active

Table 82-5 Configure Recovery MAD Status to Active

Steps	Command	Description
Enter global configuration mode	**configure terminal**	-
Configure recovery MAD status to Active	**mad restore**	Required By default, MAD is in Active status

NOTE

- When MAD status changes to Recovery, MAD will leave the ports/interfaces that have been turned off alone. When Recovery MAD status is Active, only those ports/interfaces that have been turned off by MAD will be turned on.

82.2.5 MAD Monitoring and Maintaining *-B -S -E -A*

Table 82-6 MAD Monitoring and Maintaining

Command	Description
show mad exclude recovery interface [**switchport** | **vlan**]	Display reserved interfaces that have been configured
show mad fast-hello	Display MAD Fast-Hello information
show mad lacp	Display MAD LACP information
show mad status	Display MAD status

82.3 Example of MAD Typical Configuration

82.3.1 Configure MAD LACP Function *-B -S -E -A*

Network Requirements

- Device0, Device1 form a stacking system that has Device0 as the master controller, PC1 accesses IP Network via the stacking system;
- Configure MAD LACP function, so that when Device1 splits off from the stacking

system as a result of virtualization link interface fault, PC1 can access IP network normally without giving rise to any business abnormality due to network configuration conflict.

Network Topology

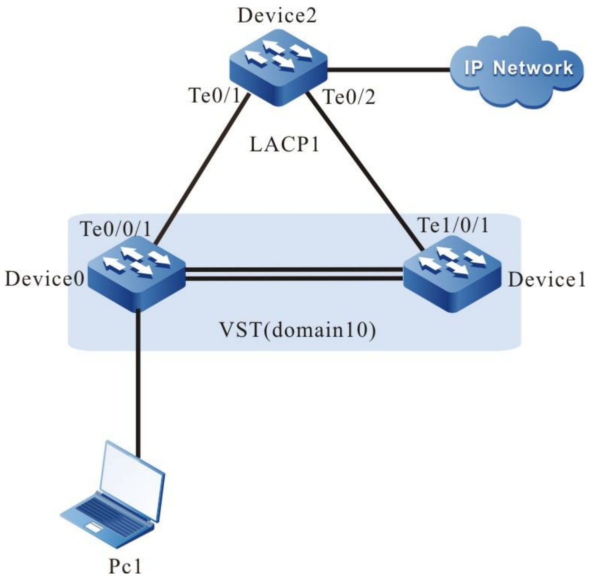


Figure 82-1 Networking Diagram - Configure MAD LACP Functions

Configuration Steps

Step 1: Make Device0 and Device1 form a stacking system that has Device0 as the master controller.

Omitted

Step 2: Configure MAD LACP function on Device0.

#On Device0, create VLAN2, and create dynamic aggregation group 1, configure aggregation group1's link type to Trunk to allow for the pass of vlan2's business.

```
Device0#configure terminal
Device0(config)#vlan 2
Device0(config-vlan2)#exit
Device0(config)#link-aggregation 1 mode lacp
Device0(config)#link-aggregation 1
Device0(config-link-aggregation1)#switchport mode trunk
Device0(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device0(config-link-aggregation1)#exit
```

#On Device0, add port tengigabitethernet0/0/1, tengigabitethernet1/0/1 to aggregation group1.

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
Device0(config-if-range)#link-aggregation 1 active
Device0(config-if-range)#exit
```

#On Device0's aggregation group1, enable MAD LACP function.

```
Device0(config)#link-aggregation 1
Device0(config-link-aggregation1)#mad enable
```

```
Device0(config-link-aggregation1)#exit
```

Step 3: Configure Device2.

#On Device2, create VLAN2, and create dynamic aggregation group 1, configure aggregation group1's link type to Trunk to allow for the pass of VLAN2's business.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#link-aggregation 1 mode lacp
Device2(config)#link-aggregation 1
Device2(config-link-aggregation1)#switchport mode trunk
Device2(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device2(config-link-aggregation1)#exit
```

#On Device2, add port tengigabitethernet0/1, tengigabitethernet0/2 to aggregation group1.

```
Device2(config)#interface tengigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 active
Device2(config-if-range)#exit
```

Step 4: Check the result.

#Check the MAD LACP information on Device0.

```
Device0#show mad lacp
------------MAD-LACP INFORMATION--------------
  Link-aggregation        Mad state
 -----------------       -----------------
       1                 enable
```

#When Device1 splits off from the stacking system as a result of virtualization link interface fault, the MAD status of the stacking system that has Device0 as the master controller will be Active, and the MAD status of the stacking system that has Device1 as the master controller will be Recovery.

```
Device0#show mad status
 MAD status: active

Device1#show mad status
 MAD status: recovery
```

#PC1 can access IP Network.

82.3.2 Configure MAD Fast-Hello Function *-B -S -E -A*

Network Requirements

- Device0 and Device1 form a stacking system that has Device0 as the master controller;
- Configure MAD Fast-Hello function, so that when Device1 splits off from the stacking system as a result of virtualization link interface fault, PC1 can access IP network normally without giving rise to any business abnormality due to network configuration conflict.

Network Topology

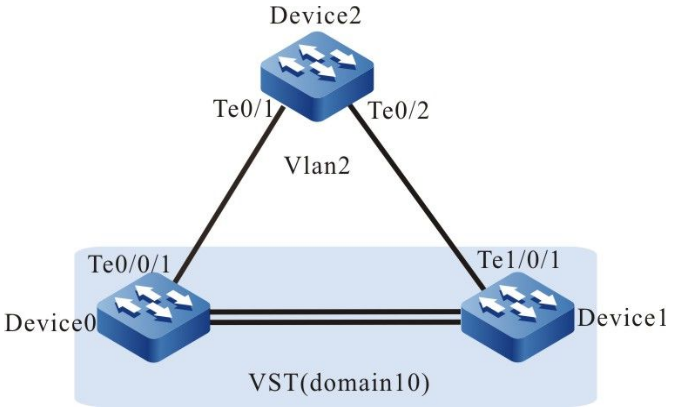


Figure 82-2 Networking Diagram - Configure MAD Fast-Hello

Configuration Steps

Step 1: Make Device0 and Device1 form a stacking system that has Device0 as the master controller.

Omitted

Step 2: Configure MAD Fast-Hello function on Device0.

#On Device0, create VLAN2, and configure it as MAD Fast-Hello's control VLAN.

```
Device0#configure terminal
Device0(config)#vlan 2
Device0(config-vlan2)#mad fast-hello control-vlan
Device0(config-vlan2)#exit
```

#On Device0, configure port tengigabitethernet0/0/1, tengigabitethernet1/0/1's link type to Trunk, and add MAD Fast-Hello's control VLAN.

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
Device0(config-if-range)#switchport mode trunk
Device0(config-if-range)#mad fast-hello vlan 2
Device0(config-if-range)#exit
```

#On Device0, turn off port tengigabitethernet0/0/1, tengigabitethernet1/0/1's STP function.

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
Device0(config-if-range)#no spanning-tree enable
Device0(config-if-range)#exit
```

Step 3: Configure Device2.

#On Device2, create VLAN2, and configure port tengigabitethernet0/1, tengigabitethernet0/2's link type to Trunk to allow for the pass of vlan2's business .

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#interface tengigabitethernet 0/1,0/2
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#exit
```

#On Device2, turn off port tengigabitethernet0/1, tengigabitethernet0/2's STP function.

```
Device2(config)#interface tengigabitethernet 0/1,0/2
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit
```

Step 4: Check the result.

#On Device0, check the enabling state of MAD Fast-Hello.

```
Device0#show mad fast-hello
 MAD Fast-Hello Information:
  Normal interval     : 2000 ms(default: 2000)
  Aggressive interval : 500  ms(default: 500)
  Aggressive duration : 120  s (default: 120)
  Control vlan        : 2
  -------------- -------------
  Interface      Control vlan
  -------------- -------------
  te0/0/1        2
  te1/0/1        2
```

#When Device1 splits off from the stacking system as a result of virtualization link interface fault, the MAD status of the stacking system that has Device0 as the master controller will be Active, and the MAD status of the stacking system that has Device1 as the master controller will be Recovery.

```
Device0#show mad status
 MAD status: active

Device1# show mad status
 MAD status: recovery
```

Appendix: Abbr. in This UM

Abbr.	Definition
AAA	Authentication, Authorization, Accounting
ABR	Area Border Router
ACL	Access Control List
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Boundary Router
BDR	Backup Designated Router
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
BSR	Bootstrap Router
CFI	Canonical Format Indicator
CFM	Connectivity Fault Management
CHAP	Challenge Handshake Authentication Protocol
CIST	Common and Internal Spanning Tree
C-RP	Candidate-Rendezvous Point
CST	Common Spanning Tree
DAI	Dynamic ARP Inspection
DHCP	Dynamic Host Configuration
DNS	Domain Name System
DoS	Denial of Service
DP	Designated Port
DR	Designated Router
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN

Abbr.	Definition
EAPOR	EAP Over RADIUS
EGP	External Gateway Protocol
ERPS	Ethernet Ring Protection Switching
ERSPAN	Encapsulated remote SPAN
FTP	File Transfer Protocol
FTPS	FTP-over-SSL
GR	Graceful Restart
HA	High Availability
ICMP	Internet Control Message Protocol
ICPIF	Impairment Calculated Planning Impairment Factor
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol snooping
IGP	Internal Gateway Protocol
IPng	IP Next Generation
IPv6	Internet Protocol Version 6
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
IST	Internal Spanning Tree
LACP	Link Aggregation Control Protocol
LACP PDU	Link Aggregation Control Protocol Data Unit
LAN	local area network
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LMP	Link Manage Protocol
MAD	Multi-Active Detection
MDIX	Media Dependent Interface Crossover
MED	Media Endpoint Discovery
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance

Abbr.	Definition
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NAS	Network Access Server
NBMA network	Non-Broadcast Multi-Access Network
ND	Neighbor Discovery
NLRI	Network Layer Reachability Information
NMS	Network Management Station
NS	Neighbor Solicitation
NSSA	Not-So-Stub-Area
NTP	Network Time Protocol
OID	Object Identifier
ORF	Outbound Route Filtering
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAP	Password Authentication Protocol
PBR	policy-based route
PIM-SM	Protocol Independent Multicast-Sparse Mode
PVID	Port VLAN ID
RA	Router Advertisement
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role Based Access Control
RIP	Routing Information Protocol
RIPng	RIP next generation
RMON	Remote Network Monitoring
RP	Rendezvous Point
RP	Root Port
RPL	Ring Protection Link
RRP	Role Resolution Protocol
RS	Router Solicitation

Abbr.	Definition
RSPAN	Remote Switched Port Analyzer
RSTP	Rapid Spanning Tree Protocol
RT	Route Target
RTR	Response Time Reporter
SFTP	Secure File Transfer Protocol /Secure FTP
SLA	Service Level Agreements
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SPT	Shortest-path Tree
SSH	Secure Shell
STP	Spanning Tree Protocol
TCN BPDU	Topology Change Notification BPDU
TCP	Transmission Control Protocol
TDP	Topology Discovery Protocol
TFTP	Trivial File Transfer Protocol
TPID	Tag Protocol Identifier
TTL	Time To Live
UDP	User Datagram Protocol
ULFD	Unidirectional Link Fault Detection
UNI/NNI	User Network Interface/ Network-Network Interface
URPF	Unicast Reverse Path Forwarding
UTC	Universal Time Coordinated
VBRP	Virtual Backup Router Protocol
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
VRRPv3	Virtual Router Redundancy Protocol Version 3
VS Domain	virtualization switching domain
VST	Virtual Switching Technology
WOL	Wake On LAN